Master's thesis

2019

Ivan Talwar

**NTNU**
Norwegian University of
Science and Technology
Faculty of Information Technology and Electrical
Engineering
Department of Information Security and Communication
Technology

Master's thesis

NTNU
Norwegian University of
Science and Technology

Ivan Talwar

# Risk Quantification to Measure Security Performance

## SecurityScore Assessment Methodology

December 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

# Risk Quantification to Measure Security Performance

SecurityScore Assessment Methodology

**Ivan Talwar**

Masters in Information Security
Submission date: December 2019
Supervisor: Laura Georg Schaffner

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

# Abstract

With the digitalisation of information, the security aspect of it has become more important than ever before. It was reported in an independent study that 7 out of 10 attacks on information assets of an organisation are carried out via their partners. Despite all the statistics, little or no attention is paid towards ensuring information security. Likewise, when two companies merge, it is the information security template of the larger party that is incoherently applied to the smaller organisation in question. Only if information security could be quantified using a universal scale, better decisions could be made while choosing the business partners like contracted vendors and new acquisitions, and better information security models irrespective of the size of the origin-organisation.

In this project, management of the top consulting firms like *KPMG and Deloitte were* consulted to establish the problem questions in conjunction with the acquisitioning or acquisitioned party. The challenges circumference around the lack of standard frameworks which hinders repeatability of the results when performed by two different organisations using their proprietary methodologies. These processes are not only expensive, time-consuming and complicated, but also completely opaque to the hosts. The methodology is a trade-secret to the conducting consultant organisations, and therefore cannot be evaluated for efficacy or relevance. Also, when large organisations invite tenders for collaborative work, the main focus is the financial numbers. No or little attention is paid towards the security posture of these contractor firms, which acts as an attack surface for future potential breaches due to shared IT platforms.

A *three-prong approach* is being proposed to remedy the situation. Each prong denotes a step towards quantifying the information security posture of an organisation. The first step is asking the rated organization to answer a questionnaire, second is to evaluate and grade them based on their answers both based on the general threat landscape, and the sector-based and third step is to provide them with relevant mitigation steps based on their security posture. These mitigation steps are to be derived from the ISO 27001 standard. For sector-specific analysis, three industry types have been piloted with, i.e. Education, Maritime and Healthcare.

These security models are framed in the form of a questionnaire and have been named *SecurityScore Assessment Methodology* that quantifies the information security posture. Then feedback is sought from them, to give direction to any future research in this area.

Some unforeseen benefits of these models include – a *benchmarking tool* which can internally be utilised by these organisations to improve their security posture, basis to evolve a *universal security scoring system* which will be easy to use and completely transparent. Additionally, insurance companies can use the security scores to decide the annual premium for the organisations choosing *insurance* as a means of *risk-transfer*.

*Information security evaluation is critical today and should be accessible to all!*

# Preface

This study is a part of the master thesis for *Norwegian University of Science and Technology* (NTNU) as a student in *Masters in Information Security (MIS)*. The idea for the thesis dawned upon me while I worked in the oil sector. As I studied various aspects of information security, the problem becomes more apparent, and the lack of study in this area makes it more relevant.

This study is aimed to draw the readers' attention towards the ever-increasing need for information security and quantification seems to be the easiest way to put across the message to the stakeholders and decision-makers. The readers do not require to possess specialised knowledge in the field of information security; however, some basic understanding is desired. It is my firm belief that this study can enable many organisations to perform in-house information security evaluation and progress from there. Also, a standard tool for information security quantification can transform the approach of the organisations towards information security on the same grounds of credit ratings.

I want to thank all the teachers who shared their invaluable knowledge and expertise with me. This enabled me to understand information security on a broader spectrum. Also, the people who participated in the study and made it possible for me to steer the study to a conclusion. To name a few – Magnus Feide (Risk Manager, Deloitte), Thijs Timmerman (Risk Manager, KPMG), Lillian Bøe Larsen (CEO, Marin IT AS), Geir Nesse (IT Manager, SIB).

I would especially extend my gratitude toward my supervisor *Prof. Laura Georg Schaffner* who enhanced my knowledge and interest towards the nitty-gritty details of information security during her course – *Security Management Metrics*. She not only imparted her specialised knowledge in the subject-matter, but also provided exposure to us by introducing us to the industry specialists and organise workshops with them. She guided me immensely in shaping up this work which would have otherwise been very hard.

*Oslo, Norway*

**14-12-2019**

# Table of Contents

# List of Figures

# List of Tables

# List of Abbreviations (or Symbols)

| | |
|---|---|
| ACL | Access control lists |
| AOI | Areas of Interest |
| AppDev | Application development |

| | |
|---|---|
| BYOD | Bring your own device |
| CA | Certificate authorities |
| CCS | Cybersecurity services |
| CIA | Confidentiality, Integrity and Availability |
| CISO | Chief Information Security officer |
| CMA | Cyber Maturity Assessment |
| CMS | Centers for Medicare & Medicaid Services |
| CSC | Cybersecurity services |
| CVSS | Common vulnerability scoring system |
| DHCP | Dynamic host configuration protocol |
| DMZ | De-militarized zone |
| DNS | Domain name service |
| ENISA | European Union Agency for Network and Information Security |
| EU | European Union |
| GDPR | General data protection regulation |
| IDS | Intrusion detection system |
| IP | Intellectual property |
| IPS | Intrusion prevention system |
| ISO | International organization for standardization |
| ISP | Internet service provider |
| KPI | Key performance indicators |
| M&A | Mergers and Acquisitions |
| MAC | Media access control |
| MPLS | Multi-protocol label switching |
| NDA | Non-disclosure agreement |
| NERC | North American electrical reliability corporation |
| NIAC | National infrastructure advisory council |
| NIST | National institute of standard and technology |
| OS | Operating system |
| OSI | Open system interconnection |
| OWASP | Open web application security project |
| P2P | Point to point |
| PDCA | Plan do check act |
| Prv- | Privileged or provisional |
| RBAC | Role-based access |
| ROI | Return on investment |
| SCADA | Supervisory control and data acquisition |
| SOC | Security operations center |
| SOP | Standard operating procedure |
| TCP/IP | Transmission control protocol |
| TPM | Trusted platform module |
| VLAN | Virtual local area network |
| XML | Extensible markup language |
| XSS | Cross-site Scripting |
| XXE | XML External Entity |

# 1 Introduction

With the digitalization of information, information security has surfaced as an area of concern across all sectors. Many solutions are available today that gives an expensive yet very generic solution to the information security concerns. While some organisations understand the repercussions of a breach, they do not act vigilantly enough while choosing their partners with whom they share access to their IT systems and valuable information.

*We are sufficiently secure and compliant* – believed the staff responsible for the information security at *Target* chain of retail stores in the USA. In 2013, they were audited and found the *Payment Card Industry Data Security Standard (PCI-DSS)* compliant (Plachkinova & Maurer, 2018). It started with a phishing attack against *Fazio Mechanical Services, Target's* refrigeration contractor (Beaver, 2014). Compromised credentials provided to *Fazio* by *Target* were used to access the network via a web portal and plant a *BlackPOS* malware at the *Point of Sale (POS)* terminals to scrape credit card information directly from the memory of these POS computers every time a card was swiped. As a result, 70 million customer records were stolen (Chapman M. , 2014). A recent study by *Opus and Ponemon* concludes that 59 percent of the companies experienced a breach caused by third-party partners (Professional Services Close - Up, 2018). When an organization decides to collaborate with an external partner, they accept their security risks too (Beale, 2017). It is interesting that during *Mergers and Acquisitions (M&A),* a similar situation arises. Interestingly, *Bloch and Zerfass* in the book *Value in Due Diligence* (Gleich , Kierans, & Hasselbach, 2010) writes about the factors considered during IT due diligence – the compatibility of the acquired systems with the inhouse systems, equipment being procured, their strategies, the IT resources and assets, but do not specifically see it as an increased attack surface. Until all the processes, hardware and software solutions are standardized (Alaranta & Mathiassen, 2014), it creates a similar vendor-client situation where the parent company will share access with the acquisition company . Also, when mergers & acquisitions occur, usually the larger shareholder supersedes the information security mechanisms of their minor shareholder firm (Larsen, 2018). Little thought is given to evaluate and adapt the better one out of the two. This cannot be blamed merely on the lack of will to do so but simply due to the lack of standardised evaluation practices (due diligence) which are usually complex and expensive to adopt and carryout (Felde, 2018). Information security standards and various models act like guiding principles to the modern-day security professionals, but there are no standards that fit the aforementioned scenarios.

There are some off-the shelf products also available like *FICO, Security Scorecard Inc., FISASCORE* etc. The problem with these solutions is the costs associated with them, their proprietary methodologies and lack of transparency (since it is their trade secret).

Some open-source solutions, like CVSS and OWASP Risk Rating systems, are freely available as discussed later in this paper, which is more software vulnerability oriented.

## 1.1 Topic covered by the project

Imagine an organisation spending millions in Information security, and yet a breach happens. Not through your network but one of their vendor's network. *Beale* from *Gartner* wrote in the *Journal of Business Continuity & Emergency Planning* (Beale, 2017) that due to a greater reliance on third party vendors, a wide range of consequences like supply-chain disruptions, vendor fraud, cyber incidents, data loss and regulatory fines have stemmed up. According to Gartner, 43 percent of organizations reported third party incidents to the board; a figure that has doubled since 2015 (Beale, 2017). The attacks against the vendors are increasing by the day (KPMG, 2018) due to the shared information resources and looser security controls at the vendor's end. It makes it important to weigh not only the financial numbers in the bid but also the information security posture of a vendor. *Game theory* for information security (Liang & Xiao, 2013) suggests that organisations with lower levels of security controls are more prone to cyber-attacks than the ones with higher levels controls. A formal quantification methodology needs to be formulated, and the results need to be added as a part of the bid to make decisions on future collaborations.

Additionally, when mergers or acquisitions occur, usually the bigger organisation uses its information security mechanisms as a draft for the smaller acquired or merged partner (Larsen, 2018). No or little effort is made (Larsen, 2018) to adapt to the smaller organisations' model of information security, even if it is better. It is mainly because the process can be cumbersome, complex and expensive (Timmerman, 2018). Also, the methodology of the consultant companies to such tasks is either opaque or translucent to protect their intellectual property.

Some of the key milestones of this research project can be outlined as:

- Search and evaluate the existing methods that could perform identical functions and their applicability in our scenarios.
- Draw the lessons from these methods or solutions and create a framework that could quantify the information security posture of an organization in a convenient manner.
- In order to form the framework, identify the key components of the IT infrastructure and security policies that reflect on the security posture of an organisation.
- Ensure that the framework that will consider all the necessary identified IT Infrastructure components, policies and incorporate the lessons learnt from the evaluation of existing solutions (verify against some established standard).
- Develop a point-based system to measure the security preparedness of an organisation in the form of a definitive, repeatable and quantitative process.
- Once created, share it with the industry professionals to test these frameworks and provide feedback to them based on their answers.
- Seek feedback from them to improve the research work.
- Look at the other possible applications of this framework.

## 1.2 Keywords

Information Security score, Mergers & Acquisitions (M&A), Vendor Risk Management, benchmarking, CVSS 3.1, OWASP Risk Rating System, OSI Model, ISO 27001, Risk quantificationIntrC, ENISA threat landscape report, energy, healthcare, education.

## 1.3 Problem description

### 1.3.1 Scenario 1

The scenario is about a client and a vendor organisation. The client floats a tender and invites bids for contract work to be done, and *Vendor A* gave a really low figure. Another firm, *Vendor B*, gave a slightly higher number. The client will be inclined to choose *Vendor A* as the big value is lower.

Some of the key issues to be considered here:

- Are the financial values in the bid the only important factor that should be weighed while deciding? What about the information security posture of these vendor organisations? According to Ng, *Commercial Manager at Halfwave AS* (Ng, 2018), information security is not the top priority, but the quality of the services is more important.
- The security posture is important because the clients will share privileged access with the vendor firms to collaborate. If the security controls are weak in the vendor firms, they will act as an attack surface that is not protected, thus creating an indirect vulnerability (Beale, 2017). Low hanging fruits are always on the target by the adversaries, as suggested by game theory (Liang & Xiao, 2013).
- Should there be an attack in the vendor firm, the client firm is automatically vulnerable to a wide range of consequential themes - physical or digital harm; economic harm; psychological harm; reputational harm; and social and societal harm (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018).

### 1.3.2 Scenario 2

The scenario encompasses a situation where two medium-sized companies (*Company X* and *Company Y*) are merging. Both feel that their Information Security technologies and policies are better than the other. Due to this sense of superiority, they feel that their IT Security technologies and policies should be used as a template to be implemented in the sister entity. Both of them hired Consultant *Company C* and *Company D,* respectively to enquire and rate the Information Security posture of their counterparts. According to Lillian Bøe Larsen (Bøe, 2018), CEO of *Marin IT AS* - a *Bergen, Norway* based venture (a division of *DOF Shipping*), she has been a part of an M&A (merger and acquisition) process (Larsen, 2018) and she felt that even though their technologies were years ahead than the acquisitioning firm, they were still forced to roll back to the older and less secure technologies and policies in the name of standardization.

Some challenges associated with this scenario:

- Could a common generic Information Security framework be used to quantify the security posture on the same scale to make an informed decision?
- Is it always possible or feasible to reckon on the current technologies in use and get insider information like SOPs, and IT Security policies and practices in a given organisation (as an outsider) during the due diligence process?
- Is it always financially viable for all organizations to outsource such due-diligence activities via external consultant companies?
- Do all consultant companies follow a standardized approach/process to analyse the security posture of an organisation?
- Can the results of these due-diligence be cross verified by other consultant firms (are the results scientifically repeatable)?

* It is noteworthy that the sought-after framework properties, as listed in *Scenario 1,* can also be used in *Scenario 2* to remedy the situation.

## 1.4 Justification, motivation and benefits

There are some methods available for quantifying information security, but each has some loophole connected to it. The commercial solutions or the consultant firms use their proprietary methods and evaluation techniques to generate security scores, but there is no industry standard as such. The idea is to identify as many aspects of an IT infrastructure and IT policies and procedures. Then create a point-based system (standard framework) that is transparent and easy to use by anybody in a given organisation (more like in a checklist format). These aspects should cover all necessary components of an IT Infrastructure and can further be verified against some industry standards like *ISO 27001, NIST 800:53, COBIT 5 etc.* to achieve validity from the get-go.

This will not only solve the problem question raised in the aforementioned two scenarios, but it has some other applications to. First and foremost, developing a universal security score system that is freely available, transparent, easy to use, and has generic as well as industry-specific applications.

If we look at the *Return on Investment* (ROI) assessment, this research can be seen as a *one-time investment*. Once prepared, more research can be done to improve the technique further. We are expected to spend 188 hours researching and preparing this report. As per *Thijs Timmerman, Senior Manager in Cyber Risk for KPMG* (KPMG, 2018) they spend somewhere between 5-50 working days to perform such an exercise each time. If we consider a working day to be 8 hours long and assume that it takes 25 days to complete this action, it accounts for 200 hours for just one project. One hundred eighty-eight hours vs two hundred hours is already looking better – however, in our case, it is to be done once. And every time, this framework will be used, it will only take a couple of hours to finish the report manually (or can be automated very easily too to save more time further). This will save organisations a load of money, and consultants a lot of time. Plus the framework can be seen as a single point of reference for both the organisations.

Additionally, based on *scenario 2 in section 1.3.2, w*hen the companies invite tenders from various vendors, they should not ONLY consider the low prices but also the security posture of a potential future partner. Reason being that the vendors will also share their systems. It has been widely observed that a vendor with a weak security posture is more vulnerable to cyber-attacks. (Beale, 2017). If this framework is applied to evaluate the security posture of the vendors, a quantifiably comparable data will be available to support the bid strength.

At the moment, there are some solutions that do a similar job and gives a score, but there are some issues associated with them:

- The methods and evaluation techniques are not available openly.
- These evaluation techniques differ from company to company.
- These evaluations are usually very expensive and time-consuming.
- These evaluations do not follow any pre-laid standard.

It can be seen in the document shared by *Security Scorecard Inc.* (Security Scorecard Inc., 2017) that states that they use 77 indicators to perform such an evaluation, but only a handful are mentioned even in the methodology document. This is because they see it as a trade secret and would not disclose it.

Similarly, Senior Risk Manager, *Thijs Timmerman,* stated that most of the security evaluation models and techniques are intellectual property (IP) of KPMG and cannot be disclosed (KPMG, 2018).

Based on the recommendations (Higgins, 2017) of the *US Chamber of Commerce* (USCC), principles were laid to draw such a robust evaluation tool which should be:

**Table 1.** Values suggested by USCC against what we seek in our framework (based on our scenario challenges in Section 1.3)

| Values suggested by USCC | Properties we seek in our framework |
|---|---|
| Transparency | Ease of understanding |
| Dispute, correction and appeal | Should be verifiable via widely accepted standards in the security community for the sake of acceptance and adoption |
| Accuracy and validation | Should be repeatable/scientific in nature |
| Model Governance | Should react to any changes made to any of the parameters while measuring the score |
| Independent | Should be free, easily available with no biases. |
| Confidentiality | |

Some other miscellaneous applications include the use of the general framework by:

- Insurance companies can use this data to decide the annual premium for the commercial entities when they use insurance as a risk-transfer measure (Banham, 2017).
- This can be used as a *benchmarking tool* to improve the overall security posture both internally and by auditing agencies.
- Can be developed as a universal *Security Score System* (similar to the credit rating system in the financial sector).

## 1.5 Research questions

This research topic is very relevant to the current scheme of things. This has a direct application in the real world.

In order to proceed with this research, the following questions need to be answered.

- What are the existing security rating methods available today to quantify information security risks (applicable to our scenarios), and what are their pros and cons?
- Can an efficient and scientifically repeatable framework be developed by learning from these methods and rating systems?
- Can the framework cover all the key components of an IT Infrastructure and set of policies that reflect on the Information Security posture of an organisation?
- Can this new point-based framework be developed in such a way that it is easy to use, transparent, and covers most of the key components and aspects of an IT eco-system in a checklist form?
- Can this framework provide a sector-specific risk assessment?
- Can this framework solve any other issues with the findings of the research?

## 1.6 Planned contribution

The master thesis research will be focused on developing a point-based framework that will aim to standardize the process of quantifying the metrics that reflect on the security posture of an organisation. This framework will cover the most important KPIs that reflect on the soundness of the information security systems and policies of an organisation.

Based on the evaluations, mitigation steps will be recommended to the participating firms to help them strengthen their information security posture.

## 1.7 Limitations

Although, the research has been planned to be very comprehensive and precise, yet there are a few foreseen limitations which can be listed as below:

- The time is a major road-block to study, collaborate, create, distribute and gather feedback to come to conclusions.
- The proposed framework needs to be shared with the industry to evaluate live environments. Many might be reluctant to share such sensitive information with a student due to the fear of exposure as well as embarrassment if they are not well prepared.
- The information is collected via Google forms and then a report is manually created with relevant mitigation steps. This process could be automated but need time and resources to create, manage and sustain.
- There is little information available publicly about the proprietary security evaluation models as these are deemed as trade secrets. Therefore, open-source scientific models have been used in conjunction with ISO standards.
- The feedback collected from the participants could not be incorporated into the solution due to the time constraint.

## 1.8 Structure of the thesis

First of all, section 2 lists various risk assessment models from the past and being used today – both open source and commercial. Gaps in these models are then concluded with the determination of some characteristics of an ideal assessment model principle using RiskM methodology (Strecker, 2011).

In section 3, the methodology to carry out the research has been explained and also the ethical considerations made during the research process.

In section 4, an assessment methodology is derived based on the literature review conducted in section 2. Then the questions in the assessment model are weighed against the ISO 27001 standard.

In section 5, conclusions are drawn with section 6 depicting the limitations and scope for further research.

# 2 Literature Review

There is a need for a standardized security posture quantification framework. The two scenarios mentioned in section 1.3, *i.e.* considering vendor as a part of the overall risk portfolio of an organization while giving them contracts and decision on adoption of security technology and policies in case of a merger or an acquisition; makes the need more reasonable. Now the questions that arise are – *i) Is there any standardized method in use across businesses to quantify overall security posture of an organization, i.e. IT Infrastructure and Policies? ii) Is it completely transparent and freely available with a sector specific evaluation? iii) Is it easy to apply and benefit from its recommendations; by anyone with basic knowledge about IT Infrastructure and policies?*

In this section, we will discuss various risk assessment models and their pros and cons. Then we will try to find the gaps in them in general based on our research problem questions. Then we will discuss the process of risk management which includes risk assessment in order to adopt appropriate risk strategy responses, i.e. risk avoidance, mitigation, transfer and acceptance (Bhoola, Hiremath, & Mallik, 2014). Subsequently, will also discuss relevant threat actors with the current threat landscape with a few selected sector-specific information. Based on those findings, we will derive the characteristics of an ideal evaluation system which answers our research questions.

## 2.1 Early Risk Assessment systems

This process of IT Risk assessment dates to 1970s. The quantitative approach relied rigorously on the mathematical modeling involving probability theory or fuzzy logic to extract a cyber-risk (CR) value (Mukhopadhyay1, Chatterjee2, Bagchi3, Kirs, & Shukla, 2019).

Risk Analysis model presented by *Courtney* in 1977 took data disclosure, modification and destruction into consideration which could be either accidental or intentional against the dollar value for every hour while the data in question is unavailable (Courtney Jr. , 1977). This model pre-dates the commercialization of computers and the evolution of the concept of threat landscape (Rifkin, 1989).

Then came along one of the first security evaluation using fuzzy metrics which was named *SECURATE* at the time; which introduced the fuzzy logic (Hoffman, Michelman, & Clements, 1978), but lacked any concrete loss estimation, threat identification mechanisms and security measures or controls (Mukhopadhyay1, Chatterjee2, Bagchi3, Kirs, & Shukla, 2019).

**Table 2.** Risk Quantification Models

| Probability-based | Fuzzy Logic |
|---|---|
| LRAM (Guarro, 1987) | RiMaHCoF (Smith & Eloff, 2002) |
| Bayesian Decision Support System (Ozier, 1989) | |
| CBBN for c-VA (Mukhopadhyay, Das, Sadhukhan, & Saha, 2013) | |

Then surfaced the *hybrid models* that comprised of a qualitative and a quantitative approach to risk assessment. *RiskPAC* (Baskerville, 1993) which utilized information from business stakeholders, IT Security, risks, audits and the business continuity/disaster recovery plans.

**Limitations in the models**

Some common issues with these models are lack of loss estimation, vulnerability assessment, threat identification, security measures and controls (Mukhopadhyay1, Chatterjee2, Bagchi3, Kirs, & Shukla, 2019).

As the technology advanced and the threat landscape evolved, many new hybrid models were developed. But none of these models managed to gain a foothold in the industry as a *gold standard*.

## 2.2 Open source Risk Rating systems

Quantified information is always easy to work with. A person without any know-how of the matter can base their decisions on numbers rather than an empirical argument (Gelbstein, 2013). When information security posture is analyzed, and concrete, repeatable values are generated, the executive management feels more confident in allocating budget in the respective mitigation projects (Gelbstein, 2013).

The concept of information security spawned in 1900 BC (Sidhpurwala, 2013) when the first use of cryptology was found in an inscription. However, with the introduction of computers, organisations started to secure their computers in the 1960s. (Lynett, 2015). We have come a long way now where every smallest vulnerability is sought after by the adversaries and can potentially be exploited. On the other hand, the defending parties are on a continuous lookout for vulnerabilities in their IT eco-system.

Organisations that have not been compromised yet and spend some money on information security tend to feel confident about their information security controls, which is a mistake (KPMG, 2014) (Firstenberg, 2016). In the context of this research, the vendor companies and the larger M&A party may also have this notion that they are good at information security. However, a quantified evaluation of their information security posture can confirm or refute the hypothesis.

In 2005, the *National Infrastructure Advisory Council (NIAC)* finished their research and CVSS Version 1 was introduced. (First.org, 2005). Ever since this business idea was floated across the industry and many businesses started with the concept of a quantified risk value. Some of the concepts are discussed below.

### 2.2.1 Common Vulnerability Scoring System (CVSS)

CVSS (Spanos, & Angelis, 2013) is one of the earliest scoring systems that was introduced by the United States government – *National Infrastructure Assurance Council (NIAC)* and furthermore, promoted by FIRST (first.org, 2019).

**Process**: It uses three metric groups – *the base, the temporal and the environmental*. The base metrics used to compute the score of CVSS are namely –

**Access vector** – Represents how the vulnerabilities can be exploited.

**Access complexity** – Measures the complexity needed to exploit a vulnerability.

**Authentication** – Reflects on authentication levels required to exploit a vulnerability.

**Confidentiality Impact** – Reflects on the impact of confidentiality breach on a system.

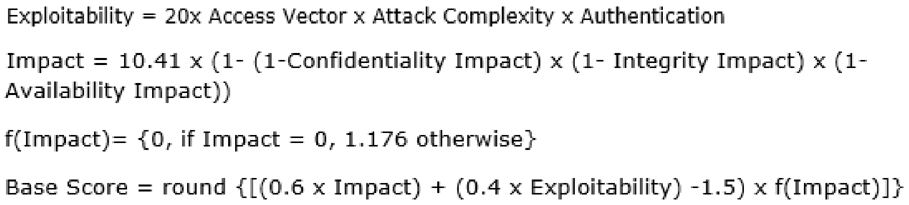
**Integrity Impact** – Reflects on the impact of compromised integrity on a system.

**Availability Impact** – Reflects on the impact on availability when a system is exploited.

**Table 3.** CVSS Metrics chart

| Metric Name | Metric Values | Metric Weights |
|---|---|---|
| Access Vector | Local, Adjacent Network, Network | 0.395, 0.646, 1 |
| Access Complexity | High, Medium, Low | 0.35, 0.61, 0.71 |
| Authentication | Multiple, Single, None | 0.45, 0.56, 0.704 |
| Confidentiality Impact | None, Partial, Complete | 0.0, 0.275, 0.660 |
| Integrity Impact | None, Partial, Complete | 0.0, 0.275, 0.660 |
| Availability Impact | None, Partial, Complete | 0.0, 0.275, 0.660 |

The base score is derived from the two sub-scores called the *Exploitability score* and *Impact score*. The first three base metrics are used to calculate the Exploitability score. The other three base metrics are used to calculate the Impact score (first.org, 2019).



Exploitability = 20x Access Vector x Attack Complexity x Authentication

Impact = 10.41 x (1- (1-Confidentiality Impact) x (1- Integrity Impact) x (1-
Availability Impact))

f(Impact)= {0, if Impact = 0, 1.176 otherwise}

Base Score = round {[(0.6 x Impact) + (0.4 x Exploitability) -1.5) x f(Impact)]}

**Figure 2.1.** CVSS 3.1 - base score (first.org, 2019)

**Pros of the model**

- The model is very flexible, elaborate and scientific.
- The quantification of the vulnerabilities can be done with precision.
- An elaborate database of CVEs national vulnerability database from NIST is used (NIST 3, 2019).
- The model is responsive to any changes made to the vectors entered for each vulnerability.

**Limitations in the model**

- More software-centric evaluation methodology where vulnerabilities are analyzed for impact analysis.
- Needs some understanding of the model, identify vulnerabilities in the software, then identify access vector, access complexity, authentication, CIA impact for each vulnerability, then some calculations based on the base scores. This process can be cumbersome and time consuming.
- The time delays between publication (Ruohonen, 2019) of *Common Vulnerabilities and Exposures* (CVEs) in the *National Vulnerability Database* (Science Direct, 2019) (NIST 3, 2019) and the CVSS information attached to published CVEs.

### 2.2.2 Open Web Application Security Project (OWASP)

*OWASP Risk rating methodology* is a model used to quantify the vulnerabilities in the software applications in the following steps (OWASP, 2019).

*Sechel* has also described the model and illustrated it with an example in detail in his paper - *Web Applications Vulnerability Management using a Quantitative Stochastic Risk Modeling Method* (Sechel, 2017).

*Step 1:* Risk will be calculated with the following formula (OWASP, 2019).

Risk = likelihood x Impact

*Step 2:* Factors for estimating likelihood on a scale of 0-9 (OWASP, 2019).

**Threat Agent factors**

*Skill level* – Nation-states (9), Cyber Criminals (7), Hacktivists (5), Students (2)

*Motive* – High (9), somewhat high (7), moderate (5), low (2)

*Opportunity* **–** No access required (9), some access required (5) full access required (0)

*Size* **–** dedicated team (9), organized yet fragmented group (6), vaguely connected group (4), individuals (1)

**Vulnerability Factors**

*Ease of discovery* – Practically impossible (1), difficult (3), easy (6), automated tools (9)

*Ease of exploit* - Theoretical (1), difficult (3), easy (5), automated tools available (9)

*Awareness* (Unknown (1), hidden (4), obvious (6), public knowledge (9)

*Intrusion* - Active detection in an application (1), logged and reviewed (3), logged without review (8), not logged (9)

*Step 3:* Factors for estimating the impact (*Business impact factors are a better measure of calculating the risk score, but sometimes this data is not available, technical impact factors are a good alternative)* (OWASP, 2019)

**Technical Impact Factors** (some numeric values assigned to each factor characteristic)

*Loss of confidentiality* **-** Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

*Loss of integrity-* Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

*Loss of availability-* Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)

*Loss of accountability-* Fully traceable (1), possibly traceable (7), completely anonymous (9)

**Business Impact Factors** (some numeric values assigned to each factor characteristic)

*Financial damage* - Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)

*Reputation damage* - Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)

*Non-compliance* - Minor violation (2), clear violation (5), high profile violation (7)

*Privacy violation* - One individual (3), hundreds of people (5), thousands of people (7), millions of people (9).

Calculation of threat agent factor, vulnerability factor, business impact and technical impact.

***Step 1:*** Based on each threat agent (*Nation-state, Cyber-criminals, Hacktivists and Students*), assign a value from 0 (lowest) to 9 (highest) to each parameter i.e. *Skill level (α), Motive (ß), Opportunity (p) and Size (q)* based on the organizations' feedback on the questionnaire. Take an average of all those values, and that will be the *Threat agent factor score (μ)* (OWASP, 2019).

$$\mathrm{\mu} = \mathrm{avg}(\alpha, ß, \mathrm{p}, \mathrm{q}) \qquad (1)$$

***Step 2:*** Based on the input, assign a value to the factors – *Ease of discovery (Þ), Ease of exploit (r), Awareness (amongst users) (s) and Intrusion (t)* on the same scale as above to calculate *vulnerability factor score* ($\mu'$) (OWASP, 2019).

$$\mu' = \mathrm{avg}(\mathrm{Þ}, \mathrm{r}, \mathrm{s}, \mathrm{t}) \qquad (2)$$

***Step 3:*** From (1) and (2);

Likelihood score, *L* = $\mathrm{avg}(\mathrm{\mu}, \mathrm{\mu}')$

Similarly, one of the *Impact scores* will be calculated, i.e. either Technical Impact or Business impact. *(Business impact factors are a better measure of calculating the risk score, but sometimes this data is not available, technical impact factors are a good alternative)*

**Pros of the model**

- The model is very flexible and easy to understand.
- The model can be customized based on the nature of the vulnerability or the threat actors.
- It gives the freedom to calculate the impact in terms of a technical impact if the business impact data is not available.

**Limitations in the model**

- It is a more software vulnerability impact analysis method. It does not apply to the matters related to other IT infrastructure related matter (*for ex*. Network security).
- Under *Impact* – it either evaluates the *business impact* or *technical impact* at once.
- For every vulnerability, one must adjust the parameters based on the *threat agent* and *vulnerability variables* which can be a complicated & time-consuming process.

## 2.3 Evolution of Commercial Risk Scoring solutions

In 2017, the *US Chamber of Commerce (USCC)* in collaboration with over 40 companies across sectors including *British Telecom, CyberGRX, Clearsky. Cisco, FICO, Goldman Sachs, Lockheed Martin, Microsoft, RiskRecon. Security 50, Security Scorecard Inc., Starbucks,* and *Verizon* defined the principles of a fair and accurate security rating system

(Higgins, 2017). This was aimed to assist cyber security professionals in the evaluation of an organizations' cyber security efforts (US Chamber of Commerce, 2017).

According to *USCC* (Banham, 2017), principles for fair and accurate security ratings include;

**Transparency** – Rating companies, shall provide transparency into the methodologies and types of *KPIs* used to determine ratings.

**Dispute, correction and Appeal** – Provision for the rated organization to challenge the rating and possibly provide revised data for re-evaluation.

**Accuracy and Validation** – Ratings should be empirical, data-driven, or as an expert opinion. Rating organizations should provide validation of their methodologies and the historical performance of their models.

**Model Governance** – Should there be any changes in the evaluation models, should provide information to the customers in advance and the reasons for the change.

**Independence** – These ratings should be unbiased irrespective of any trade associations or collaborations with the rated organization.

**Confidentiality** - Information provided by the rated organization shall be appropriate safeguarded.

After these principles were introduced, there are some *off the shelf* products like *FICO, FISAScore, Security Scorecard Inc*. that provide generic scaling platforms, but they are very opaque in their methods and expensive too.

### 2.3.1 Security Scorecard, Inc.

A white paper was issued by them in 2017 that gives us a fair bit of an idea of how this rating system works (Security Scorecard Inc., 2017)

**Process**: It states that Security Scorecard Inc. grades the cyber security health of an organisation based on the information collected by their proprietary search engine, *ThreatMarket. Banham* (Banham 2, 2017) described that the *ThreatMarket* is used to collect and correlate terabytes of proprietary security information from around the world. The platform assesses the strength of an organization's cyber security plans, and benchmarks these plans against those of other companies. A scale of A to F is used. The sources are usually data feeds, sensors, honeypots, sinkholes etc. This data is weighted based on the severity, risk levels, and benchmarking within the industry (Security Scorecard Inc., 2017) using the *ThreatMarket* data.

Issues are graded by Risk Factors. There are 77 issue types recognized by *Security Scorecard*. All issues are not weighed as equal but are based on the severity of the impact. The severity of the problem is then calculated using quantifying standards such as *CVSS 2.0* (NIST, 2016). The greater the likelihood ratio, the more predictive the factor of the breach is.

These scores are indicative of the current security posture and change periodically as the threat landscape evolves. If there are any vector changes, they reflect in two weeks, should the organisation is using their platform, or if Security Scorecard is logging a firm based on their IPV4 data.

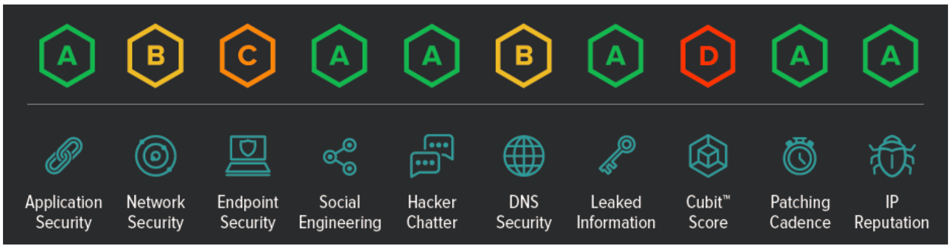


**Figure 2.2** Issues graded by Risk factor

**Pros of the model**

- Elaborate examination of the aspects of IT infrastructure – 77 different parameters used for the rating (Security Scorecard Inc., 2017).
- ThreatMarket engine is trained by terabytes of data; which makes it mature and probably gives it an edge over other proprietary solutions (Banham 2, 2017).
- The security metrics are regularly updated to adapt to the evolving threat landscape.

**Limitations in the model**

- Lack of transparency in the information about *issue types (KPIs in the SecurityScore)* which makes it hard to understand.
- Calculates risk scores against the information provided by *ThreatMarket*; a proprietary instrument of Security Scorecard Inc. is (Banham 2, 2017).
- If the threat landscape changes and the risk calculation methodology is altered, it takes 2 weeks to reflect on the risk assessments (Security Scorecard Inc., 2017).
- The solution implementation requires fund allocation in the budget and therefore, needs to be planned way ahead in time. For some organizations, it is not possible to buy such a solution due to lack of funds.
- This method is suggestive of what is vulnerable in the network by scoring various aspects of the infrastructure. However, it does not define the exact point of failures and some suggestive mitigation steps.
- Last but not the least, it does not consider the overall risk portfolio, as recommended (Korolov, 2017), of the rated organization (including vendors, suppliers and other third-party allies).

### 2.3.2 FISAScore

It is a numeric value cumulative high-risk score assigned to an organisation based on the information security assessment indicative of critical vulnerabilities, control strength inefficiencies, and other relevant threats to an organisation (FrSecure, 2019) It encompasses around *ISO/IEC, COBIT5, CCS, CSC, NERC and the NIST Cyber Security Frameworks*. These are utilized to underline the best practices and create a baseline for the entire evaluation process.

**Process**: This framework has the following four phases that thoroughly run through the current practices of an organisation to generate a security score.

*Administrative Controls*: Inspects and measures the 'human' aspect of information security like policies, awareness training, guidelines, standards and procedures.

*Physical Controls*: Measures the level of physical security controls to safeguard the information assets like access terminals, camera surveillance, alarm systems etc.

*Internal Technical Controls*: As suggested by the name, these are technical in nature and are observed inside of an organisation. Some examples are firewalls, IPS/IDS, endpoint security, mobile device management etc.

*External Technical Controls*: These are technical controls but observed outside of an organisation like search engine indexes, DNS, open ports, vulnerability scanning etc.

A minimum of 300 (poor) and a maximum of 850 (good) is obtained post-evaluation using FISAScore methodology of system security assessment.

**Pros of the model**

- Elaborate factors – administrative, physical, internal and external controls; which covers a wide range of vulnerabilities.
- Inspired by well known information security standards that improve the level of trust of the rated organization in the model.

**Limitations in the model**

- Complete lack of transparency in the methods used for scoring.
- No information on what it calculates and if there are any mitigation suggestions against the evaluates points. Only broad categorization like Administrative controls, Physical Controls, Internal technical controls, and external technical controls are available.
- Does not calculate the overall risk portfolio, including the vendors, as suggested by *Korolov* (Korolov, 2017).
- May not be cost-feasible for some organizations.

Banham in his 2017 article *Investing in the Insurtech Toolbox* for *Risk Management New York* journal mentioned a few more risk quantification platforms (Banham 2, 2017) like;

### 2.3.3 RiskIQ

It provides a unified view of rated organizations' digital assets and risks to it. Additionally, it monitors employees' web, mobile and social media activities to map it against attack vectors used by hackers by using their proprietary algorithms. (Banham 2, 2017).

**Pros of the model**

- Assists in gaining a good overview of the digital assets of the organization.
- Real time monitoring can trigger a real time response to any ongoing attempt to compromise the IT infrastructure.
- Due to the progressive nature of the algorithm (machine learning), the model will get better over the period of time as more data is fed into it.

**Limitations in the model**

- The obvious flaw in the plan is the invasive nature of the inspection.
- Plus it seems to focus more on insider threat and
- Heavy dependency on the algorithm can be problematic as maturity and training methods of this algorithm are unknown.

### 2.3.4 Cyence

It models the financial impact of different types of cyberattacks, helping insurance companies understand the risk probabilities for different insured products (Banham 2, 2017).

**Pros of the model**

- An effective tool for the insurance companies to see through the risk profile of the organization and thereby charge them accordingly for transferred risks.
- Additionally, CISOs can use the same model to verify the insurers' claims.

**Limitations in the model**

- Mainly interested in finding the financial impact of a potential incident.
- Based on historical data to predict future attacks; not the best approach with the constantly changing threat landscape.

## 2.4 Gaps in the models from sections 2.2 and 2.3

As discussed in the section for problem questions, there are many gaps in the currently available models.

- The open source models are very software vulnerability-centric and cannot be applied to the overall IT Security posture of an organization.
- The open source models are customizable but need to be adjusted for each vulnerability being evaluated.
- The open source models are a bit technical and complicated and need prior knowledge of the models in order to carry out the evaluations.
- The commercial (off the shelf products) are not transparent in terms of modus operandi for security score calculation. When asked about some cybersecurity evaluation models, Senior Risk Manager for *KPMG Nordics, Thijs Timmerman*, stated that most of the security evaluation models and techniques are intellectual property (IP) of KPMG and cannot be disclosed (KPMG, 2018).
- Since these products have limited transparency, it is hard to tell if all critical factors of success to evaluate the information security performance were considered (*Table. 1*). Additionally, it is hard to verify the scientific properties and repeatability of the results. Therefore, rated organizations are left with no other option but to trust the results.
- Each model has its own mechanism to quantify information security, and therefore there is no standardized method utilized across the businesses.
- The commercial (off the shelf products) requires an extensive investment which might not be feasible for all organizations.
- The commercial (off the shelf products) evaluates the security preparedness with a quantified number but does not recommend what to do to mitigate those problems. Further investments would be needed to buy additional services to mitigate the discovered issues.
- None of the models mentioned above provides a sector-specific risk assessment.
- *Banham* (Banham, 2017) raised a very relevant point to our studies. He pointed out that cybersecurity rating firms attempt to calculate the rated company's cumulative risk as a simple score, much on the lines of a personal credit score. However, it does not account for outside suppliers, vendors, cloud providers and other third external partners. *Korolov* also points at the absolute need to add the

third-party risk factors in the overall risk portfolio of an organization (Korolov, 2017). *Korolov* also points at the absolute need to add the third-party risk factors in the overall risk portfolio of an organization (Korolov, 2017).

## 2.5 Risk Management

*International Organization of Standardization (ISO)* defines Information Security Management as (ISO/IEC 27001, 2013);

"a systematic approach to managing sensitive company information to maintain its security. It includes people, processes and IT systems by applying risk management processes."

In the past, assessment of IT-related risks was focused on determining tangible (physical) IT assets, internal and external threats to those assets, and the vulnerability of these assets (Rainer Jr., Snyder, & Carr, 1991). But a more contemporary definition suggests that IT risks pervade organizations from IT Operations to Corporate Strategy (Westerman & Hunter, 2007). Due to increasing attacks on organizations, the IT Risk assessment scope has widened to the entire organization – its institutions and actors, their responsibilities, and intangible assets such as employee details and information assets (data) (Gerber & Solms, 2005). The risk assessment process evaluates the risks to IT technologies used to store the data and the policies that govern the flow of data.

According to *Tudor* in his book - *Information Security Architecture* (Tudor, 2000), there are five components for any information security architecture:

- Organization and IT infrastructure
- Security policy, standards and procedures
- Security baselines and risk assessments
- Security awareness and training programs; and
- Compliance

*Govindaraju, Akbar and Suryadi* define *IT Infrastructure* to be composed of Physical hardware (like servers, storage systems, printers, hubs, switches, routers, etc.), platforms and IT applications (Govindaraju, Akbar, & Suryadi, 2018). A similar definition is suggested by *Hsu* - *A Dictionary of Business and Management in China* (Hsu, 2018).

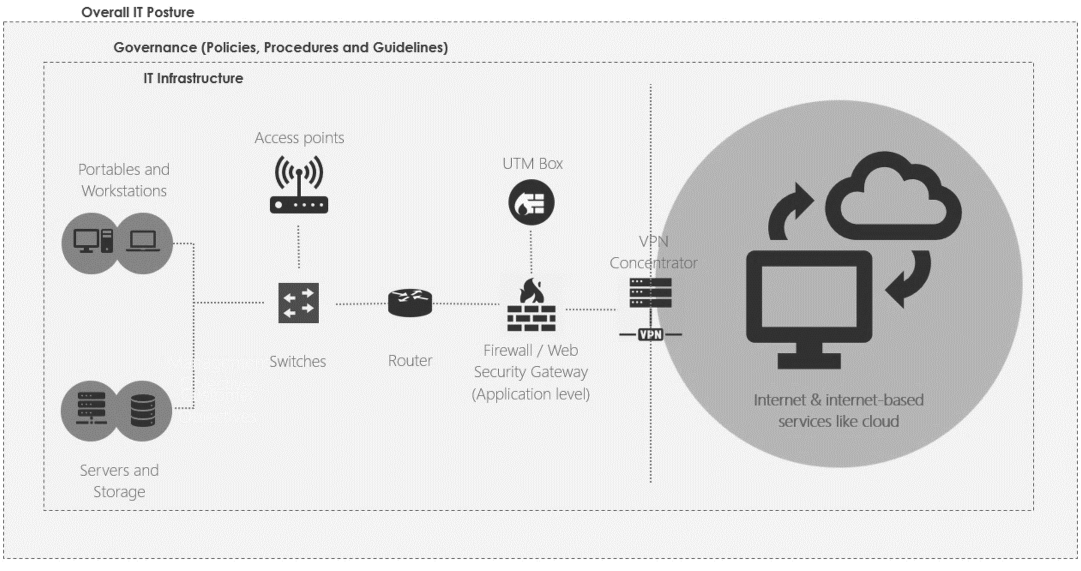

Overall IT Posture
Governance (Policies, Procedures and Guidelines)
IT Infrastructure
Access points
Portables and Workstations
UTM Box
VPN Concentrator
VPN
Switches
Router
Firewall / Web Security Gateway (Application level)
Internet & internet-based services like cloud
Servers and Storage

**Figure 2.3.** Typical IT Setup

It is further elaborated by the *ISO/IEC 17799* (Hong, Chi, Chao, & Tang, 2003) (ISO/IEC 17799, 2005) that provides the scope of information security management:

- information security policy establishment and assessment;
- information security organization and responsibility;
- personnel security management and training;
- computer system security management;
- network security management;
- system access control;
- system development and maintenance security management;
- information assets security management;
- physical and environment security management; and
- business planning and management.

*Also*, ISO/IEC 27001:2013* describes in detail which all components to secure under the Information Security Management System in its *Annexure A* (ISO/IEC 27001, 2013).

*Dulaney and Stinson,* in their book *CompTIA Security+ Deluxe Study Guide* (Dulaney & Stinson, 2011) has divided the security controls into three categories:

**Management Controls** – Risk Assessment, Planning, System & Service Acquisitions, Certification, Accreditation & Security Assessment.

**Operational Controls** – Personnel Security, Physical & Environmental Security, Contingency Planning, Configuration Management, Maintenance, System & Information Integrity, Media Protection, Incident Response, Awareness & Training.

**Technical Controls** – IAM (Identity Access Management), Access Controls, Audits & Accountability and System & Communication Security.

*Bernik and Prislan* (Bernik & Prislan, 2016) has defined the following as the *critical success factors* in their *10 by 10 Model for Holistic State Evaluation*;

- Physical information security controls
- Technical and logical security controls
- Information resources management
- Employee management
- Information risk management and incident handling
- Organizational culture and top management support
- Information security policy and compliance
- Security management maturity
- Third-party relationships
- External environment connections

*IoT reference layered architecture model* (Bartosz, et al., 2018) also provides a good overview of all the factors that constitute the scope of the risks to be assessed:

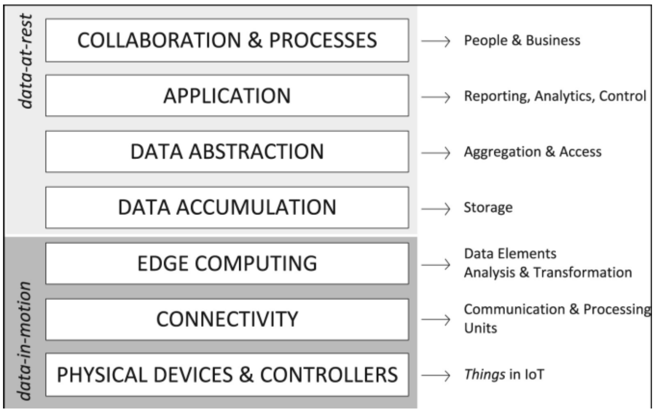

data-at-rest
data-in-motion
COLLABORATION & PROCESSES
APPLICATION
DATA ABSTRACTION
DATA ACCUMULATION
EDGE COMPUTING
CONNECTIVITY
PHYSICAL DEVICES & CONTROLLERS
People & Business
Reporting, Analytics, Control
Aggregation & Access
Storage
Data Elements Analysis & Transformation
Communication & Processing Units
*Things* in IoT

**Figure 2.4.** Internet of Things referenced layered architecture

*Angraini, Megawati and Haris* in their research paper - *Risk Assessment on Information Asset an academic Application Using ISO 27001 (* (Angraini, Megawati, & Haris, 2018) identified assets in the following categories:

**Hardware** – Workstations (PC), Servers, Network

**Software** – Applications (both *in-house and stocked*)

**Data** – information, access controls on them etc.

On top of that, risk management policies in the form of *business processes* (Angraini, Megawati, & Haris, 2018).

Based on *Tudor's* recommendations (Tudor, 2000), *Dulaney and Stinson* security control categorization (Dulaney & Stinson, 2011), ISO/IEC 17799:2005 recommendations ( (ISO/IEC 17799, 2005), the *10 by 10 model for holistic state evaluation* (Bernik & Prislan, 2016), *IoT reference layered architecture model* (Bartosz, et al., 2018), and *Angraini, Megawati and Haris'* asset identification categories (Angraini, Megawati, & Haris), the categorization of the *critical success factors* for information security posture evaluation can be streamlined to the following components:

**Table 4.** Suggested Critical success factor categories (derived from models discussed above)

| Categories | Components |
|---|---|
| *Storage* | On Premise or on cloud |
| *Servers* | Identity Management, DNS, DHCP, Application, License etc. |
| *Networks* | Internal Segmentation, routing and firewalls |
| *Information Management* | Access controls, role-based access, data classification, etc. |
| *Business Processes* | IT Security Policy, Incident Management Policy, Business Continuity, Disaster Recovery, etc. |
| *Applications* | Secure by design, patching, updates, regulatory compliance etc. |

**Note**: In order to probe the effectiveness of the controls in relation to these factors, we can use ISO 27001:2013 (ISO/IEC 27001, 2013) standard that has a set of detailed controls lists under *Annex A (normative).* This is not to be done to be compliant with ISO/IEC 27001 standard, but just to validate if the controls are in line with the ISO standard recommendations.

## 2.6 Threat Actors and Threat Landscape

### 2.6.1 Threat Actors

According to *NIST SP 800-30 standard* (NIST, 2012) and *Federal Information Processing Standard Publication FIPS PUB 200* ( (NIST 2, 2005), a *threat* is;

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

A *threat actor* is an individual or a group posing a threat.

*Bruijne, Eeten, Gañán, & Pieters* has further elaborated the definition (Bruijne, Eeten, Gañán, & Pieters, 2017)

an individual or conglomerate of individuals who (intend to)attack information systems which will harm the confidentiality, integrity, and availability of information (systems) in the Netherlands.

*Seebruck* has depicted the threat actor types in his "circular order circumplex of hack types" model (Seebruck & , 2015) based on their motive and sophistication.

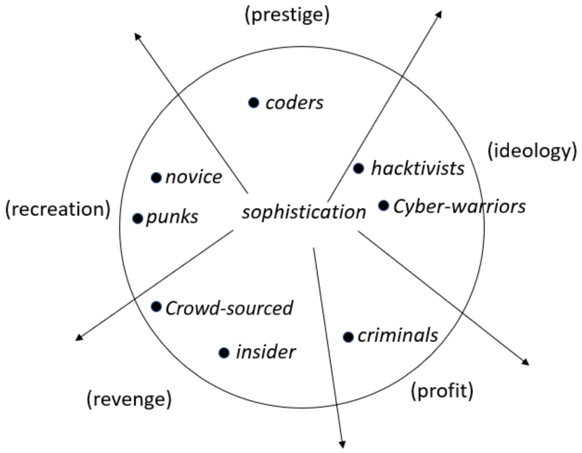


**Figure 2.5.** A circular order circumplex of hacker types **(Seebruck & , 2015)**

*Bruijne, Eeten, Gañán, & Pieters* have categorized threats & motives against private organizations, governments and citizens in their *Threat Matrix* able (Bruijne, Eeten, Gañán, & Pieters, 2017). However, our focus of the study is private organizations; we will streamline the information.Table 5. **Threat Matrix** (Bruijne, Eeten, Gañán, & Pieters, 2017)

| **Source of the threat** | **Private Organizations** |
|---|---|
| *Professional criminals* | Theft and publication or selling of information |
| | Manipulation of information |
| | Disruption of IT |
| | IT Takeover |
| *State Actors* | Digital espionage |
| | Offensive cyber capabilities |
| *Terrorist* | Disruption/Takeover of IT |
| *Cyber vandals and script kiddies* | Theft of information |

| | |
|---|---|
| *Hacktivists* | Theft and publication or selling of information |
| | Defacement |
| | Disruption of IT |
| | IT Takeover |
| *Internal Actors* | Theft and publication or selling of information |
| | Disruption of IT |
| *Cyber researchers* | Receiving and publishing information |
| *Private Organizations* | Information theft (industrial espionage) |
| *No actor* | IT Failure |

*Rieb, Gurschler & Lechner* in their paper – *A gamified approach to Explore techniques of Neutralization of Threat Actors in Cybercrime* (Rieb, Gurschler, & Lechner, 2017) have identified *Cyber criminals, Employees, Hacktivists, Nation states and Script kiddies* as the threat actors.

*European Union Agency for Network and Information Security* (ENISA) in *ETL 2018 (pg. 124)* (ENISA, 2019) defined threat agents as *cyber-criminals, insiders, nation states, corporations, Hacktivists, cyber-terrorists and script kiddies*.

*Canadian Centre for Cyber Security* (CCCS), a division of *Government of Canada*, defines the threat actors based and link them to their primary motivation (Canadian Centre for Cyber Security, 2018) – *Nation-states'* motivates are geopolitical, *cybercriminals* work for profit, *Hacktivists* have ideological grounds, *terrorists* are motivated by ideological violence, *thrill seekers* seek satisfaction, and *insider threat* act up due to discontent.

### 2.6.2 Threat Landscape

According to *Pirc, DeSanto, Davison and Gragido* in their book *Threat Forecasting*, the Threat landscape is often compared to a high stakes game of whac-a-mole: just as one mole-like threat is fixed; another one pops up (Pirc, DeSanto, Gradigo, & Davison, 2015). Cyber security is important across sectors, but we have picked up a few to illustrate the sector-wise threat landscape.

#### 2.6.2.1 **Healthcare**

ENISA has recognized the assets in the *healthcare sector* as remote care medical systems, networked implanted devices, tracker identification devices (via RFID tags etc.), networking equipment (such as routers, switches, cables, wireless equipment, computers), mobile client devices, data and physical facilities. (ENISA 4, 2018). Since the systems in a hospital setup are interconnected, the threats identified are the following:

**Malicious actions** – malware, hijacking, DoS attacks, device tampering, social engineering (phishing), theft of devices, theft of data, skimming. (ENISA 4, 2018)

**Human errors** – Resulted from the human actions leading to damaged healthcare systems. (ENISA 4, 2018)

**System Failures** – Software or firmware failure, device failure, network failure, insufficient maintenance, overloading. (ENISA 4, 2018)

**Supply Chain failure** – Cloud provider's default risk portfolio (Cloud Security Alliance, 2017), network provider, power supply provider or manufacturer of medical devices. (ENISA 4, 2018)

Relevant threat actors here may be *Nation states, cyber criminals, hacktivists, and cyber terrorists*.

#### 2.6.2.2 **Education**

There has been an increase in the number of attacks against the educational institutes lately. According to a recent paper by the *Higher Education Policy Institute* (HEPI) in the UK (Chapman D. , 2019), there are following threats in the education sector;

Nation states are targeting the **sensitive intellectual property** of the universities.

**Sector wide networks** like *Janet Network* in the UK (like *Uninett* in Norway) is being targeted to camouflage their traces by cybercriminals. (Chapman D. , 2019)

Cybercriminals are constantly seeking to steal **employees' and students' personal information and financial information** via phishing. (Chapman D. , 2019)

Hacktivists try to deface and disrupt (Bandara, Ioras, & Maher, 2014) the **university web resources** related to student education as a means of protest. (Chapman D. , 2019)

Students find vulnerabilities in the systems and try to disrupt the **integrity of data like their grades**, etc. (Chapman D. , 2019)

Relevant threat actors here are *nation-states, cybercriminals, hacktivists and script-kiddies*. (Chapman D. , 2019)

#### 2.6.2.3 **Maritime**

ENISA, in their report, reveals that there is a lack of focus on cyber security in the Maritime sector. This can be attributed to the complexity of the maritime ICT environment, fragmented maritime governance context, inadequate consideration of cyber security factors in the regulations and lack of overview of IT risk in the maritime sector (ENISA 2, 2011). However, the recent white paper issued by *World Shipping Council and other collaborating agencies* (BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, 2019), they have cleared stated the threats and associated threat actors on page 9 of the literature:

Nations states and Terrorist groups are believed to gain knowledge (**trade secrets**) and disrupt the **economy** and **national critical infrastructure**.

Criminals aim to steal **data**, launch ransom ware attacks against data systems, arrange fraudulent transportation on cargo, intelligence gathering for more sophisticated attacks in future. Their motive is believed to be financial gains, commercial and industrial espionage.

Hacktivists aim to destroy data, steal and disclose **confidential information**, cause a denial of service attacks to gain media attention or deface an organization or sector.

## 2.7 Characteristics of the desired framework

### 2.7.1 RiskM Modeling method

Strecker, in his paper *RiskM: A multi-perspective modeling method for IT risk assessment* (Strecker, 2011) has very elaborately defined the characteristics of an effective IT Risk assessment method in the form of six requirements:

#### 2.7.1.1 **Multiple Perspectives (P1)**

A method should provide perspectives into the risk specific to (groups of) stakeholders involved in the group process. The perspective may correspond with the abstractions, concepts and pictorial representations and should bring value and understanding to the targeted stakeholders. All perspectives, when combined, should present an integrated picture. (Strecker, 2011)

#### 2.7.1.2 **Organizational Context (P2)**

A method should account for both IT-related risks and chances and link them to the surrounding action system composed of all relevant organizational entities such as corporate goals, organizational units, and business processes. (Strecker, 2011)

#### 2.7.1.3 **Multiple Organizational Levels (P3)**

A method should account for cause-and-effect relationships of IT risks and chances at multiple organizational levels, from IT operations to business processes to effects on value chains and the organization as a whole. (Strecker, 2011)

#### 2.7.1.4 **Quantitative Values and Qualitative Descriptions (P4)**

A method should provide means for risk quantification where possible and means for qualitative risk description where quantification is either not feasible or not economically justifiable. (Strecker, 2011)

#### 2.7.1.5 **Compliance (P5)**

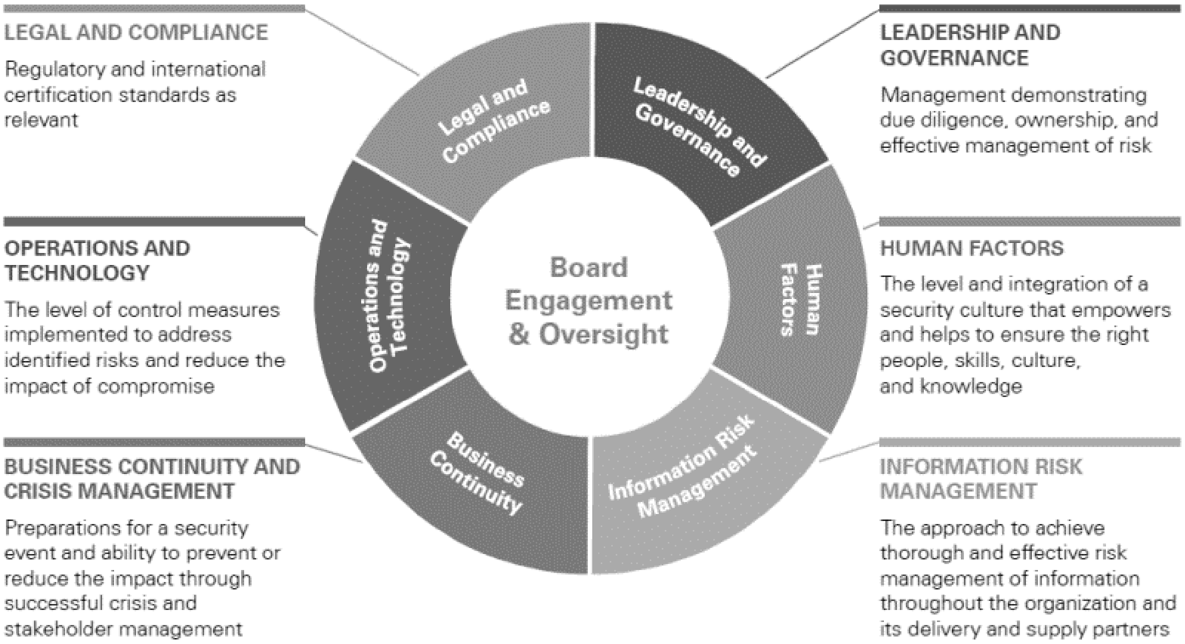
A method should support compliance validation and auditing procedures, e.g., by representing the concepts built into regulations, standards and frameworks such as COBIT, or by (possibly partially automated) validation of internal controls. (Strecker, 2011)

#### 2.7.1.6 **Multiple Phases (P6)**

A method should account for the multiple phases of the IT risk assessment process and facilitate transitions between phases, as from IT risk identification to risk analysis. (Strecker, 2011)

### 2.7.2 Probing the Critical Success Factors (from table 4)

*Critical success factor categories* to analyze and evaluate the security posture of an organization were identified in Table 4 as *Storage, Servers, Networks, Information Management, Business Processes, and Applications.* In order to probe the various aspects of security from these factors, we can use KPMG's *Cyber Maturity Assessment (CMA)* Model (Anthony for KPMG, 2015) as presented at ISACA Kenya Annual Conference.



LEGAL AND COMPLIANCE
Regulatory and international certification standards as relevant
LEADERSHIP AND GOVERNANCE
Management demonstrating due diligence, ownership, and effective management of risk
OPERATIONS AND TECHNOLOGY
The level of control measures implemented to address identified risks and reduce the impact of compromise
HUMAN FACTORS
The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture, and knowledge
BUSINESS CONTINUITY AND CRISIS MANAGEMENT
Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management
INFORMATION RISK MANAGEMENT
The approach to achieve thorough and effective risk management of information throughout the organization and its delivery and supply partners
Legal and Compliance
Leadership and Governance
Operations and Technology
Board Engagement & Oversight
Human Factors
Business Continuity
Information Risk Management

**Figure 2.6.** KPMG Cyber Maturity Assessment Model **(Anthony for KPMG, 2015)**

### 2.7.2.1 **Leadership and Governance**

This reflects on the seriousness of the top management towards Information Security (Lidster & Rahman, 2018). They should lead by example and portray a security-conscious attitude.

The following indicators can indicate that:

- A set of comprehensive information security policies in place in the organisation. (Loots, 2001)
- Policies reviewed periodically – keeping the organization's mission and vision in mind in addition to the stakeholder's expectations. (Doherty & Fulford, 2006)
- Dedicated annual budget for Information Security in addition to an emergency provision, should there be an emergency. (Weishäup, Yasasin, & Schryen, 2018)
- Dedicated workforce allocated to ensure information security – Security Operation teams (SOC), Chief information security officer (CISO), Data Privacy officers etc. (Hooper & McKissack, 2016)
- The top-level management understands their Information security *risk appetite* and has a clear roadmap to mitigate the most critical security related issues eventually. (Meirkhanova, 2019)

### 2.7.2.2 **Information Risk Management**

- This reflects on the risk management of information within the organisation as well as external partners. (Korolov, 2017)
- Due diligence while choosing a potential partner for work – can be external vendors too for short term or long-term collaboration. (Banham, 2017) (Korolov, 2017)
- Policies for handling information the workplace – confidential information not to be placed openly on the desks. (ISO/IEC 27001, 2013) (Isabella, 2008).
- Only concerned people to have access to documents or information that are confidential in nature. Various clearance levels (inspired by concepts like Bell LaPadula, etc.) can be introduced within the organisation. (O'Hara & Malisow, 2017)

- Secure print enabled on printers so that documents are only printed when the person printing them is available. (Isabella, 2008)
- A platform is available to all employees that allows them to send in their concerns related to mishandling or flawed processes around information management in the organisation. These concerns should be resolved on a case-by-case basis. (Koivunen, 2010)
- The systems holding some critical information (servers, etc.) are not physically accessible by the employees (Banerjee, Venkatasubramanian, Mukherjee, & Gupta, 2012) (ISO/IEC 27001, 2013).

#### 2.7.2.3 **Operation and Technology**

The control measures in place to address the identified risks and decrease the impact of an event (Takamura, Mangum, Wasiak, & Gomez-Rosa , 2015)

- *Access Control Management*: Access to information to be given to only the relevant employees. Techniques like Attribute based access (ABAC) or RBAC (role-based access control) are efficient and easy to use and maintain. (John, Sural, & Gupta, 2017)
- *User account termination*: To periodically check if some account has been accidentally left active. The severity of the matter can be greater if it is provisional access (meant to give access to server and other IT Infrastructure management resources). (ISO/IEC 27001, 2013)
- *Efficient and effective Incident Management*: Every incident is separately reported and assessed (Liu & Lee, 2012). This can lead to the realization of other related but more serious flaws in system security. (Taylor, Olstam, Nernhardsson, & Nitsche, 2017).
- *Patch Management*: The operating systems need security updates to be regularly installed. There should be periodic dedicated patch windows where new OS security patches can be rolled out both on workstations as well as servers (More, Stieber, & Liu, 2016).
- *No Internet access on servers*: This measure ensures that these servers are not accessible from the outside too. They can only communicate with other internal resources (that are explicitly allowed to do so) to prevent any unauthorized access (Park, Noh, Kim, & Kang, 2017).
- *Bring your own device (BYOD) Policy*: The users are not allowed to bring their own personal devices but only use the company provided equipment (Olalere, Abdullah, Mahmod, & Abdullah, 2016).
- *Whole disk/media encryption* on the workstations. (BitLocker on Windows using the TPM module) (Stephenson, 2012).
- Whole disk/media encryption on cellphone devices. (Stephenson, 2012).
- Multiple-factor authentication is used while remotely accessing the systems on the network (Olalere, Abdullah, Mahmod, & Abdullah, 2016)
- All systems – server and workstations are equipped with an *effective anti-malware* application (Wood, 2016).
- Users do not have administrator rights on local machines. (Instablogs, 2010)
- Additional security measures like file-level signature-based md5 check to look out for any known malicious file and explicit approval to run a file. (Fangyong, Hongjun, & Nong, 2009).

- In-house apps are inspired by the ‘Privacy/Secure by design’ concept (Schneider, 2018) (GDPR Peras, 2018).

#### 2.7.2.4 **Human Factors**

Humans are the weakest link in the security scheme of things. This reflects on the level and integration of a security culture that ensures the right people, skills, culture and knowledge.

- A very sound Information Security culture in the organisation (Mahfuth, Yussof, Baker, & Ali, 2017)
- Special attention is given to training the IT users in the organisation with the help of training and awareness campaigns. (D'Arcy, Hovav, & Galletta, 2009).
- Special vetting process at the time of hiring of the employees by a neutral third party (Bartlett, 2014).
- Keenly observe the employees to track any tell-tell signs of an insider threat. (Greitzer, Purl, Leong, & Sticha, 2019)
- Launch pseudo phishing attacks and check how aware the employees are – when it comes to responding to such threats on a daily basis. (Dodge, Coronges, & Rovira, 2012)
- At the time of hiring, the employees understand – any NDA (non-disclosure agreements) that they sign and follow it during the time of their employment. (Fanimokun, 2012)

#### 2.7.2.5 **Business Continuity and Disaster recovery plan**

This reflects on the preparedness of an organisation, should there be an incident that disrupts the entire operation of the business (Aleksandrova, Aleksandrov, & Vasiliev, 2018).

- A comprehensive and reliable backup solution that is not physically located close to the main systems. (Aleksandrova, Aleksandrov, & Vasiliev, 2018) (Snedaker & Rima, 2014)
- Multiple datacenters – to improve accessibility and ensure availability (Snedaker & Rima, 2014)
- A comprehensive plan ready to move the operations to an operational base and continue work from there until the primary systems/location is back online.
- A comprehensive disaster recovery plan ready to ensure that data-driven businesses can continuously carry out their work (IDC Survey: Downtime Costs Large Companies Billions, 2015).
- An ideal situation is an annual DR drill where all IT teams participate and ensure operation on the backup system. This can also be used to realize the impact of an incident, should there be any (in terms of data loss, etc.) (Snedaker & Rima, 2014)
- Post-incident analysis capabilities and procedures laid out in the organisation (Snedaker & Rima, 2014).

#### 2.7.2.6 **Legal and Compliance**

This is used to ensure that the organisation follows all the national and international laws applicable to them.

- Annual IT security audits can reflect on the overall well-being of an organisation (Enaw & Check, 2018).
- The policies and procedures should be able to stand in the court of law.

- Data privacy laws – like *GDPR in EU* should be properly implemented and abided by (Fang, 2018) (Enaw & Check, 2018) (Snedaker & Rima, 2014).
- If certified with any industry-standard certification, should be periodically reviewed to maintain the status and the certification. (Snedaker & Rima, 2014).

Additionally, as per the fifth property (P5), i.e. *Compliance* of Strecker's RiskM principles ( (Strecker, 2011), we can also validate our probing questions on the critical success factors (from Table 4) to see if we are asking the right questions. The primary goal is not to get certified against this standard, but to follow the guidelines provided by an industry standard. ISO/IEC 27001 is one of the well-recognized standards across the industry and therefore, we will use it.  The Annex A of ISO/IEC 27001 standard *(see table 14)* provides a detailed description of what controls are to be adopted to ensure the security of the information assets and the systems that these reside on (ISO/IEC 27001, 2013).

# 3 Methodology

The nature of the research is based on a hybrid approach – a combination of *qualitative* as well as a *quantitative* approach, or mixed approach.

The medium of data gathering:

- Interviews
- Literature review
- Past-experience in the industry
- Questionnaire

## 3.1 Collection

At stage 1, interview questions were sent to the management of top IT Security consultant companies (Timmerman, 2018) (Felde, 2018). This was to establish the validity of the problem questions. Since the problem question is divided into two scenarios, top leadership involved in an M&A process was also consulted (Larsen, 2018). The questions were framed and aimed to draw the light on the research topic to which respondents answered based on their perception of the items. Their real-life experiences from working in the industry were a testimony to the fact that the problems addressed in this paper are valid.

At stage 2, when the problem was clearly established – an extensive literature review was performed to form the basis for the solution of the research problem. Some of the relevant models were evaluated along with their pros and cons, and general gaps were listed. Then more about threats and threat landscape (both in general and sector-specific) were explained. Based on the problem questions, characteristics of the desired framework were established. Past-experience in the industry assisted tremendously as the basis for technologies and their purpose, and the policies are loosely generic. With qualitative research, the data collection, dissemination, processing and drawing inferences is a non-systematic and an ad-hoc process (Leedy & Ormod, 2019). However, the effectiveness of using a *mixed-method approach* has been well established.

As *Johnson, Onwuegbuzie and Tuner* said (Johnson, Onwuegbuzie, & Turner, 2007);

> "Mixed methods research is an intellectual and practical synthesis based on qualitative and quantitative research; it is the third methodological or research paradigm. It recognizes the importance of traditional quantitative and qualitative research but also offers a powerful third paradigm choice that often will provide the most informative, complete, balanced, and useful research results." (Johnson, Onwuegbuzie, & Turner, 2007)

At stage 3, the information gathered from the literature review and past-experience in the field formed the basis of a framework. Then a questionnaire was created that would not only cover the problem questions in general but in a sector-wise manner too. The rated organizations do not have to provide any additional data to be evaluated on the basis of the sector. The same data will be used to evaluate general security posture and sector-based exposure too.

At stage 4, finally, the questionnaire was approved by the supervisor and was shared with the target audience in different sectors to collect data.

## 3.2 Processing

The data collected in *Stage 1* were analyzed and aligned to establish the problem questions. It was, however, observed that one of the respondents took the scope even a step ahead when he mentioned the issue of mistrust between merging companies about their respective intellectual properties. However, another respondent claimed that some due-diligence was done before their company was acquired by a bigger organization. Yet, the better policies and newer technologies in use in the smaller organization was never adopted by the larger organization which was a step backwards for them. These factors assisted in strengthening the periphery of the research questions.

Literature review strengthened the understanding of the structure of an IT Infrastructure and governance policies driving it. Additionally, when combined with past observations while working in the same field of work, it acted as a multi-layered concept building around the problem questions. There might be a human-bias in concluding facts, but even machine learning is prone to deviations based on its prior knowledge in the area (Shepperd, 2015).

Based on the compound knowledge accumulated in the previous steps, a framework was created. The structure follows a Two-Prong approach – both for generic analysis and the sector-specific analysis. In the pilot, three sectors have been picked, i.e. maritime, education and healthcare. However, the same model can be extended to other industries as well.

Data collected during the final stage from the questionnaire were analyzed. A security score was given to the participants with some suggestions on mitigation to improve their information security posture.

## 3.3 Validation, or triangulation

At first, multiple sources were used to triangulate the validation of problem questions. Then various sources of information (literature review, interviews, questionnaires, experiments, etc.) were studied to form the basis of knowledge to furtherer conduct this study. These framework questions were further validated by widely accepted *ISO 27001* standard (ISO/IEC 27001, 2013). Then my supervisor, *Laura Georg Schaffner*, validated the framework before it was sent to the target audience.

Last but not least, a feedback loop was also created to extract participants' feedback which can be useful in improving this model in future.

## 3.4 Ethical Considerations

Ethical factors were at the core of this study.

- Consent in writing was taken while collecting sensitive information from the organizations participating in the research.
- An assurance was provided to these organizations about the deletion of the data once the purpose of the research is fulfilled.
- Individuals were explicitly asked if they would like to be anonymized in the citations.
- No work or data has been plagiarized or taken undue credit for.
- At all points during the study, any sort of bias was avoided, and the point that was put-forth was always scientifically backed.
- Whenever a dilemma arose, triangulation methods were used to proceed with the research.
- No personally identifiable information (PII) was collected during the study.

- This model will stay available to the organizations without any costs to the small organizations for preliminary security checks and benchmarking purposes.
- The research material is being submitted to the *Department of Information Security and Communication* of *Norwegian University of Science and Technology (NTNU)*. The research work is the intellectual property of NTNU.

Before the university can publish the work, the information will be sanitized to ensure that it cannot be traced back to any individual.

# 4 Discussion

There have been some gaps in the research or solutions provided so far when it comes to our research questions. We have characterized the critical success factors in table 4 and a set of characteristics of the desired model in section 2.7. *KPMG's CMA Model* (Anthony for KPMG, 2015) is used to probe the critical success factors that reflect on the security posture of an organization. *ISO 27001* standard will be used for the sole purpose of validation of questions in the study. The aim is not to certify an organization against the *ISO 27001* standard (ISO/IEC 27001, 2013). The proposed model can be called – *SecurityScore* Assessment.

## 4.1 Scope of the Model

As concluded in Section 2.5, the most typical aspects of an IT Infrastructure and the business processes; also stated as critical success factors for security performance review are *storage, servers, networks, information management, policies (business processes) and applications*.

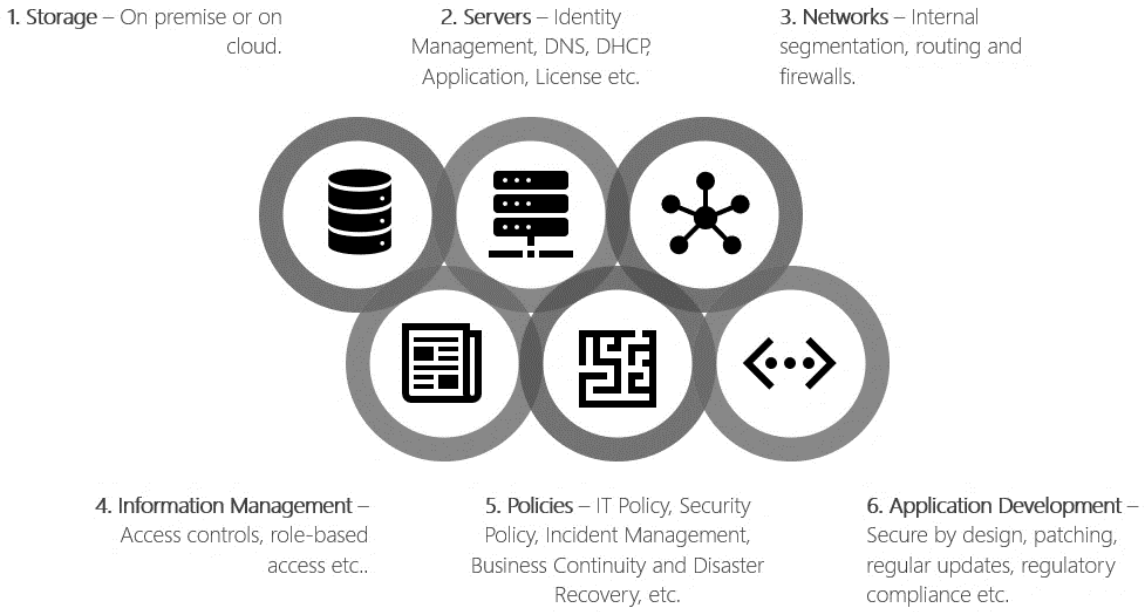

1. Storage – On premise or on cloud.
2. Servers – Identity Management, DNS, DHCP, Application, License etc.
3. Networks – Internal segmentation, routing and firewalls.
4. Information Management – Access controls, role-based access etc..
5. Policies – IT Policy, Security Policy, Incident Management, Business Continuity and Disaster Recovery, etc.
6. Application Development – Secure by design, patching, regular updates, regulatory compliance etc.

**Figure 4.1.** *Critical success factors* for assessing security performance

## 4.2 What aspects to check from the scope

By using the *KPMG's Cyber Maturity Assessment* model (Anthony for KPMG, 2015), we will probe the six *critical success factors* for assessing the security performance as discussed in section 2.7.2.

The six dimensions are *Leadership and Governance, Human Factors, Information Risk Management, Operation & Technology, Business Continuity & Disaster Recovery and Legal & Compliance,* as discussed in section 2.7.2. This provides a 360 overview of all aspects of information security controls in an organization and will help immensely in probing the critical success factors from table 4.

**Table 6.** Key questions to probe *Critical Success Factors* for assessing Security posture (table 4)

| **Dimension from KPMG's CMA** | **Aspects to probe** (section 2.7.2.1 – 2.7.2.6) |
|---|---|
| Leadership and Governance | Clear overview of assets, detailed information security policy (Loots, 2001), clearly defined roles and business functions (Hooper & McKissack, 2016), good overview of risk appetite (Meirkhanova, 2019), sufficient budget allocations (Weishäup, Yasasin, & Schryen, 2018), business processes to do due diligence for future partnerships (Banham, 2017) (Korolov, 2017), Non-Disclosure agreement with employees and partners |
| Human Factors | Security awareness amongst the employees (D'Arcy, Hovav, & Galletta, 2009), random security checks (via methods like pseudo-phishing attacks), information about security laws and regulations, the vetting process for employment (Bartlett, 2014) |
| Information Risk management | Classification of data (O'Hara & Malisow, 2017), proper access controls (John, Sural, & Gupta, 2017), Business Contingency Plan/Business continuity Plan, Disaster recovery plans in place, Policies on creating, storing and sharing of information, secure data applications |
| Operation & Technology | A good overview of assets, endpoint protection, network segmentation, network traffic analysis, intrusion detection and prevention systems, access controls, back up of data, encryption, redundancy of systems for availability and performance, encrypted, remote network access (VPN) |
| Business Continuity and Disaster Recovery | Business Contingency Plan (IDC Survey: Downtime Costs Large Companies Billions, 2015), Disaster recovery drills, multiple layers of backup (Aleksandrova, Aleksandrov, & Vasiliev, 2018) (Snedaker & Rima, 2014), Business continuity plans (to run the business out of an alternate location), elaborate Incident Management policy (Aleksandrova, Aleksandrov, & Vasiliev, 2018) (Snedaker & Rima, 2014) |
| Legal & Compliance | Compliant to data privacy laws (Fang, 2018) like GDPR – systems, applications, websites etc., a mechanism to report incidents to the authorities within the allowed time, Internal and External IT audits (Enaw & Check, 2018), periodic renewal of certifications (Doherty & Fulford, 2006) |

## 4.3 Collaborated information - *SecurityScore Assessment*

Strecker's RiskM modelling method (Strecker, 2011)recommendations, as described in section 2.7.1, can be used to check the structure of *SecurityScore assessment* (proposed method).

**Table 7.** RiskM Modeling method against proposed *SecurityScore Assessment methodology*

| ***RiskM* model recommendation** | **Proposed *SecurityScore Assessment* properties** |
|---|---|
| Multiple Perspective | Since *KPMG's CMA model* is being used, it keeps in mind the perspectives of all the stakeholders – Top management, IT teams and employees (*See table 6*) |
| Organization context | SecurityScore Assessment will query all aspects of the organization relevant to information security. |
| Multiple organizational levels | All levels are participants and hold their responsibility – top management for understanding the risk portfolio, IT Team to instate controls and employees to conform. |
| Quantitative values and qualitative descriptions | SecurityScore will quantify the security posture of an organization, but the mitigation recommendation will be qualitative. |
| Compliance | ISO/IEC 27001 will be used to verify the validity of the questions in the proposed SecurityScore Assessment. |
| Multiple Phases | The first phase will be an evaluation of the overall security posture with a questionnaire, then replying with generic score and analysis in sector-specific context and lastly some mitigation suggestions (based on the evaluation).<br>Also, the SecurityScore assessment itself will be re-evaluated periodically due to the changing threat landscape. |

Based on the critical success factors of success for assessing security performance (*see table 4*) , KPMG's Cyber Maturity Assessment Model (Anthony for KPMG, 2015) and RiskM Modeling methodology (Strecker, 2011), the following questions should probe the overall security posture of an organization. These questions are a part of the proposed *SecurityScore Assessment* methodology.

### 4.3.1 Business Processes (general policies)

**Table 8.** Framework questions about the General Policies

| **Nr.** | **Framework Questions** |
|---|---|
| 1. | Do you have a clear overview of all the IT assets (Asset Management) that exist in the organisation (including but not limited to the SCADA devices)? |
| 2. | Do you have any pre-defined Information security policy to ensure the confidentiality, integrity and availability of the information systems? |
| 3. | Do you have dedicated Information Security roles as in a CISO or a Data Privacy Officer in your organisation? |
| 4. | Do you have a dedicated team working to detect and respond to security incidents – Security Operations Center (SOC) or an Incident Response Team (IRT)? |
| 5. | Do you have a dedicated annual Information Security budget in your organisation? |
| 6. | Does your top management know about the organisation's risk appetite and is actively engaged in making a roadmap for the future? |
| 7. | Do you have a provision of an emergency fund in case of an event – to mitigate the issue on an emergency basis? |
| 8. | Do you perform due diligence on the information security posture of your future business partners or vendors? |

| | |
|---|---|
| 9. | Do you have a strict policy against bringing your own device and connected it to the organisation network? |
| 10. | Does your organisation use multi-factor authentication? |
| 11. | Do you have a policy for issuing time-bound credentials to the guest Wi-Fi network? |
| 12. | Do all the workstations have a malware protection program installed? |
| 13. | Do the users have local administrator right on the workstations? |
| 14. | Do you conduct regular user training and awareness campaigns to minimize security breaches that involve a human error? |
| 15. | Do you periodically send out pseudo-phishing emails to your own IT users to check their knowledge and preparedness against such attempts? |
| 16. | Do you perform vetting on the new employees – background check, security check, etc.? |
| 17. | Do you have any dedicated channels to report any possible insider threat? |
| 18. | Do you make the new employees sign an NDA (Non-disclosure agreement) to ensure that all the trade secrets are kept safe?) |
| 19. | Do you have annual IT Audits to benchmark your systems/practices or to retain security certifications? |
| 20. | Do you have policies that can withstand in the court of law? |
| 21. | Do you have full compliance with the local laws of the land like GDPR, Data Privacy Law, etc.? |
| 22. | Is there a Business contingency plan in place in the event of an incident? |
| 23. | Do you have a Disaster Recovery protocol or a mechanism in place, should there be an incident? |
| 24. | Do you perform Disaster recovery drills on an annual basis where all the stakeholders (teams) participate and check their capability to resume activity should there be an incident? |

### 4.3.2 Network

**Table 9.** Framework questions about Network

| Nr. | Framework Questions |
|---|---|
| 25. | Do you have Virtual LANs (VLANs) set up on the switches for different devices? (For example – separate VLANs for workstations, printers, Wi-Fi, servers, video solutions etc.) |
| 26. | Do you have MAC tagging enabled on the switch ports giving internet access to employees performing key functions like payroll, HR, finance etc.? |
| 27. | Do you have 802.1x protocol enables at the port level to force user authentication whenever the data passes through the port? |
| 28. | Do you have an Access Control List (ACL) or any other form of routing table configured on your router to dynamically assess and filter the data traffic? |
| 29. | Do you use internal DNS servers to route your network traffic? |
| 30. | Do you have a network firewall that filters the data traffic by allowing and disallowing data traffic based on the pre-defined set of rules? |
| 31. | Do you have a web security gateway that can inspect even the content of the data packets to make a decision on whether to allow or disallow a data packet? |
| 32. | Do you have a stateful inspection firewall that keeps a record of any communication between an internal and an external host and can allow or disallow communication requests based on that historical data? |

| | |
|---|---|
| 33. | Do you have a load balancing provisions enabled in your infrastructure on the assets being frequently used by the users to ensure availability? |
| 34. | Do you have VPN concentrators to form encrypted VPN tunnels from outside of the network? |
| 35. | Do you have VPN set up on the router / firewall level to allow secure external connection to the internal network? |
| 36. | Do you have an Intrusion detection system (IDS) to detect any malicious activity on the internal network? |
| 37. | Do you have an automated response system should a malicious activity is detected (Intrusion Prevention System)? |
| 38. | Do you use any Protocol Analyzers like Wireshark to monitor the network traffic between points of interests (ex - a user connects to a confidential internal database, etc.)? |
| 39. | Does your network equipment filter traffic based on the validity of security certificates of a website, i.e. revoked certificate websites are not accessible? |
| 40. | Do you have an encrypted connection (tunnel) to any external network (which can be a sister company or a business partner) configured at the router level? |
| 41. | Do you use an MPLS connection for data traffic that needs to be transmitted on a real-time basis? |
| 42. | Do you have special security measures in place for internet-facing services (for example a demilitarized zone or a DMZ)? |

### 4.3.3 Storage

**Table 10.** Framework questions about Storage

| Nr. | Framework Questions |
|---|---|
| 43. | Do you have a backed-up copy of all the data stored on the network resources at all times? |
| 44. | Do you have redundancy of the storage units – in datacenters or on the cloud to ensure recoverability in case of an event? |
| 45. | Do you have physical security at the places where the storage equipment is kept? |
| 46. | Do you have other forms of security controls (like access cards, biometric scans, etc.) to ensure the safety of the storage equipment? |
| 47. | Is the data stored locally on computers and on file servers encrypted – disk encryption (for example with BitLocker)? |
| 48. | Is the data (media) stored on the cellphones encrypted? |
| 49. | Do you have video surveillance available for the places where storage equipment is stored? |
| 50. | Do you have provisions for logging user activity and storing it while they access these storage devices? |

### 4.3.4 Servers

**Table 11.** Framework questions about Servers

| Nr. | Framework Questions |
|---|---|
| 51. | Do all the servers have internet access? |
| 52. | Do you have malware protection installed on the servers? |

| | |
|---|---|
| 53. | Do you have any other form of intrusion detection system available on the servers that would raise a security flag, should there be any malicious activity detected? |
| 54. | Do you have processes to periodically check if the user accounts have been properly terminated once an employee leaves? It is very important in case of provisional (prv) accounts with elevated access.*)* |
| 55. | Do the servers have any controls that block the installation of new programs on the servers (for example – Carbon Black which needs an explicit approval on the checksum value of every file being executed)? |
| 56. | Do you have redundant servers to ensure availability and disaster recovery? |
| 57. | Do you have an OS patch management system in place – installing security patches during a maintenance window to ensure the safety of the systems? |
| 58. | Do you have separate types of user accounts – one to access workstation and other provisional accounts to access infrastructure management resources like servers? |
| 59. | Is multiple-factor authentication enabled to access the servers remotely?*)* |

### 4.3.5 Applications

**Table 12.** Framework questions about Applications

| Nr. | Framework Questions |
|---|---|
| 60. | Do you have an application development team to maintain and update the in-house applications? |
| 61. | Do you program in-house application using "secure by design" approach? |
| 62. | Are these applications regularly updated considering the changing threat landscape? |
| 63. | Are these applications tested for any vulnerabilities from the security point of view (techniques like penetration testing, risk assessment, etc.)? |

### 4.3.6 Information Management

**Table 13.** Framework questions about Information Management

| Nr. | Framework Questions |
|---|---|
| 64. | Do you have a good overview of the information assets that you possess? |
| 65. | Do you have good access control mechanisms in place so that only authorized employees can access the information? |
| 66. | Have you differentiated the information based on the criticality like terming documents are classified, confidential, private, de-classified etc. (following some model like Bell-LaPadula, Chinese wall, etc.)? |
| 67. | Do you have a clear desk policy – where the confidential information is not kept openly on the desk for others to be seen? |
| 68. | Do you have other confidentiality measures like secure printing – the print job will be finished only when the person physically shows up at the printer? |
| 69. | Do you use any other form of document control system like SharePoint, box, Google drive etc. for version control, collaboration or integrity check? |

70. Do you have a system in place where the users can report any incidents related to mishandling of the information at a workplace (classified documents lying on the printer etc.) to be addressed on a case-by-case basis?

## 4.4 Validation of the questions against ISO 27001 standard

As the principle – Compliance of the RiskM modeling method suggests (Strecker, 2011), we can verify if the questionnaire is in line with an industry standard. As discussed in table 7, we will use ISO/IEC 27001 as a benchmarking tool (ISO/IEC 27001, 2013) using the elaborate Annex A.

Annex A (normative) (ISO/IEC 27001, 2013) defines the *reference control objectives and controls* in great detail. Summarized points about the annexure.

**Table 14.** ISO 27001 Annex A (summary)

| | **Reference Control Objectives** | **Controls** |
|---|---|---|
| A.5 | Information Security Policies | 1. Management direction for information security |
| A.6 | Organization of information security | 1. Internal organization<br>2. Mobile devices and teleworking |
| A.7 | Human resource security | 1. Prior to Employment<br>2. During Employment<br>3. Termination and Change of Employment |
| A.8 | Asset Management | 1. Responsibility of assets<br>2. Information Classification<br>3. Storage Media handling |
| A.9 | Access Control | 1. Business requirements of access control<br>2. User access management<br>3. User responsibilities<br>4. System and application access control |
| A.10 | Cryptology | 1. Cryptographic controls |
| A.11 | Physical and environmental security | 1. Secure areas<br>2. Equipment |
| A.12 | Operations Security | 1. Operations procedures and responsibilities<br>2. Protection for Malware<br>3. Backup<br>4. Logging and Monitoring<br>5. Control of operational software<br>6. Technical vulnerability management<br>7. Information system audit considerations |
| A.13 | Communication Security | 1. Network security management<br>2. Information transfer |
| A.14 | Security acquisition, development and maintenance | 1. Security requirements of information systems<br>2. Security in development and support processes<br>3. Test data |
| A.15 | Supplier relationships | 1. Information Security in supplier relationships<br>2. Supplier service delivery management |
| A.16 | Information Security Incident Management | 1. Management of information security incidents and improvements |

| | | |
|---|---|---|
| A.17 | Information Security aspects of business continuity management | 1. Information security continuity<br>2. Redundancies |
| A.18 | Compliance | 1. Compliance with legal and contractual requirements<br>2. Information security reviews |

### Validation of SecurityScore Assessment methodology against ISO 27001 standard

**Table 15.** Framework questions about the *business processes* **(ISO/IEC 27001, 2013)** *and (see table 14)*

| Nr. | Framework Questions | Supported by |
|---|---|---|
| 1. | Do you have a clear overview of all the IT assets (Asset Management) that exist in the organisation (including but not limited to the SCADA devices)? | (*ISO/IEC 27001 Annex A.8.1.1)* |
| 2. | Do you have any pre-defined Information security policy to ensure the confidentiality, integrity and availability of the information systems? | (*ISO/IEC 27001 Annex A.5.1.1)* |
| 3. | Do you have dedicated Information Security roles as in a CISO or a Data Privacy Officer in your organisation? | (*ISO/IEC 27001 Annex A.6.1.1)* |
| 4. | Do you have a dedicated team working to detect and respond to security incidents – Security Operations Center (SOC) or an Incident Response Team (IRT)? | (*ISO/IEC 27001 Annex A.6.1.2)* |
| 5. | Do you have a dedicated annual Information Security budget in your organisation? | (*ISO/IEC 27001 Annex A.17.1.1)*<br>(*ISO/IEC 27001 Annex A.5.1.1)*<br>(*ISO/IEC 27001 Annex A.6.1.5)*<br>(*ISO/IEC 27001 5.1.c)* |
| 6. | Does your top management know about the organisation's risk appetite and is actively engaged in making a roadmap for the future? | (*ISO/IEC 27001 5.1.a & b)*<br>(*ISO/IEC 27001 6.1.2)* |
| 7. | Do you have a provision of an emergency fund in case of an event – to mitigate the issue on an emergency basis? | (*ISO/IEC 27001 5.1.c)* |
| 8. | Do you perform due diligence on the information security posture of your future business partners or vendors? | (*ISO/IEC 27001 6.1.2)* |
| 9. | Do you have a strict policy against bringing your own device and connected it to the organisation network? | (*ISO/IEC 27001 Annex A.6.2)*<br>(*ISO/IEC 27001 Annex A.8.1)* |
| 10. | Does your organisation use multi-factor authentication? | (*ISO/IEC 27001 Annex A.9.4.2)* |
| 11. | Do you have a policy for issuing time-bound credentials to the guest Wi-Fi network? | (*ISO/IEC 27001 Annex A.12.1.1)*<br>(*ISO/IEC 27001 Annex A.9.4)*<br>(*ISO/IEC 27001 Annex A.9.2.1)* |
| 12. | Do all the workstations have a malware protection program installed? | (*ISO/IEC 27001 Annex A.12.1.1)* |
| 13. | Do the users have local administrator right on the workstations? | (*ISO/IEC 27001 Annex A.9.2.2)*<br>(*ISO/IEC 27001 Annex A.9.2.3)* |

| | | |
|---|---|---|
| 14. | Do you conduct regular user training and awareness campaigns to minimize security breaches that involve a human error? | *(ISO/IEC 27001 Annex A.16.1.6)*<br>*(ISO/IEC 27001 7.2)*<br>*(ISO/IEC 27001 Annex A.7.2.2)* |
| 15. | Do you periodically send out pseudo-phishing emails to your own IT users to check their knowledge and preparedness against such attempts? | *(ISO/IEC 27001 Annex A.12.2)*<br>*(ISO/IEC 27001 Annex A.14.2.8)* |
| 16. | Do you perform vetting on the new employees – background check, security check, etc.? | *(ISO/IEC 27001 Annex A.7.1.1)* |
| 17. | Do you have any dedicated channels to report any possible insider threat? | *(ISO/IEC 27001 Annex A.7.1.2)*<br>*(ISO/IEC 27001 Annex A.16.1)* |
| 18. | Do you make the new employees sign an NDA (Non-disclosure agreement) to ensure that all the trade secrets are kept safe?*)* | *(ISO/IEC 27001 Annex A.7)*<br>*(ISO/IEC 27001 Annex A.13.2.4* |
| 19. | Do you have annual IT Audits to benchmark your systems/practices or to retain security certifications? | *(ISO/IEC 27001 Annex A.18.2)*<br>*(ISO/IEC 27001 Annex A.12.7)* |
| 20. | Do you have policies that can withstand in the court of law? | *(ISO/IEC 27001 Annex A.18.1)* |
| 21. | Do you have full compliance with the local laws of the land like GDPR, Data Privacy Law, etc.? | *(ISO/IEC 27001 Annex A.18.1)* |
| 22. | Is there a Business contingency plan in place in the event of an incident? | *(ISO/IEC 27001 Annex A.17.1)* |
| 23. | Do you have a Disaster Recovery protocol or a mechanism in place, should there be an incident? | *(ISO/IEC 27001 Annex A.17.1)*<br>*(ISO/IEC 27001 Annex A.17.2)* |
| 24. | Do you perform Disaster recovery drills on an annual basis where all the stakeholders (teams) participate and check their capability to resume activity should there be an incident? | *(ISO/IEC 27001 Annex A.17.1.3)* |

**Table 16.** Framework questions about *Network* **(ISO/IEC 27001, 2013)** *and (see table 14)*

| Nr. | Framework Questions | Supported by |
|---|---|---|
| 25. | Do you have Virtual LANs (VLANs) set up on the switches for different devices? (For example – separate VLANs for workstations, printers, Wi-Fi, servers, video solutions etc.) | (ISO/IEC 27001 Annex A.17.1)<br>(ISO/IEC 27001 Annex A.13.1.3) |
| 26. | Do you have MAC tagging enabled on the switch ports giving internet access to employees performing key functions like payroll, HR, finance etc.? | (ISO/IEC 27001 Annex A.13.1.3) |
| 27. | Do you have 802.1x protocol enables at the port level to force user authentication whenever the data passes through the port? | (ISO/IEC 27001 Annex A.13.1.3)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 28. | Do you have an Access Control List (ACL) or any other form of routing table configured on your router to dynamically assess and filter the data traffic? | (ISO/IEC 27001 Annex A.13.2.1) |
| 29. | Do you use internal DNS servers to route your network traffic? | (ISO/IEC 27001 Annex A.13.2.1) |
| 30. | Do you have a network firewall that filters the data traffic by allowing and disallowing data traffic based on the pre-defined set of rules? | (ISO/IEC 27001 Annex A.13.2.1) |

|  |  |  |
|---|---|---|
| 31. | Do you have a web security gateway that can inspect even the content of the data packets to make a decision on whether to allow or disallow a data packet? | (ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 32. | Do you have a stateful inspection firewall that keeps a record of any communication between an internal and an external host and can allow or disallow communication requests based on that historical data? | (ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1)<br>(ISO/IEC 27001 Annex A.13.2.2) |
| 33. | Do you have a load balancing provisions enabled in your infrastructure on the assets being frequently used by the users to ensure availability? | (ISO/IEC 27001 Annex A.17.2.1) |
| 34. | Do you have VPN concentrators to form encrypted VPN tunnels from outside of the network? | (ISO/IEC 27001 Annex A.14.1.2)<br>(ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 35. | Do you have VPN set up on the router / firewall level to allow secure external connection to the internal network? | (ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 36. | Do you have an Intrusion detection system (IDS) to detect any malicious activity on the internal network? | (ISO/IEC 27001 Annex A.13.1.2) |
| 37. | Do you have an automated response system should a malicious activity is detected (Intrusion Prevention System)? | (ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 38. | Do you use any Protocol Analyzers like Wireshark to monitor the network traffic between points of interests (ex - a user connects to a confidential internal database, etc.)? | (ISO/IEC 27001 Annex A.13.1.2) |
| 39. | Does your network equipment filter traffic based on the validity of security certificates of a website, i.e. revoked certificate websites are not accessible? | (ISO/IEC 27001 Annex A.10.1.2) |
| 40. | Do you have an encrypted connection (tunnel) to any external network (which can be a sister company or a business partner) configured at the router level? | (ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 41. | Do you use an MPLS connection for data traffic that needs to be transmitted on a real-time basis? | (ISO/IEC 27001 Annex A.13.1.2)<br>(ISO/IEC 27001 Annex A.13.2.1) |
| 42. | Do you have special security measures in place for internet-facing services (for example a demilitarized zone or a DMZ)? | (ISO/IEC 27001 Annex A.13.1.3) |

**Table 17.** Framework questions about *Storage* **(ISO/IEC 27001, 2013)** *and (see table 14)*

| **Nr.** | **Framework Questions** | **Supported by** |
|---|---|---|
| 43. | Do you have a backed-up copy of all the data stored on the network resources at all times? | (ISO/IEC 27001 Annex A.13.3.1) |
| 44. | Do you have redundancy of the storage units – in data centres or on the cloud to ensure recoverability in case of an event? | (ISO/IEC 27001 Annex A.17.2.1)<br>(ISO/IEC 27001 Annex A.13.3.1) |
| 45. | Do you have physical security at the places where the storage equipment is kept? | (ISO/IEC 27001 Annex A.11.1) |

|  |  |  |
|---|---|---|
| 46. | Do you have other forms of security controls (like access cards, biometric scans, etc.) to ensure the safety of the storage equipment? | (ISO/IEC 27001 Annex A.11.1) |
| 47. | Is the data stored locally on computers and on file servers encrypted – disk encryption (for example with BitLocker)? | (ISO/IEC 27001 Annex A.10.1.1) |
| 48. | Is the data (media) stored on the cellphones encrypted? | (ISO/IEC 27001 Annex A.10.1.1)<br>(ISO/IEC 27001 Annex A.8.3.3) |
| 49. | Do you have video surveillance available for the places where storage equipment is stored? | (ISO/IEC 27001 Annex A.11.1) |
| 50. | Do you have provisions for logging user activity and storing it while they access these storage devices? | (ISO/IEC 27001 Annex A.11.1)<br>(ISO/IEC 27001 Annex A.12.4.1)<br>(ISO/IEC 27001 Annex A.12.4.2) |

**Table 18.** Framework questions about *Servers* **(ISO/IEC 27001, 2013)** *and (see table 14)*

| Nr. | Framework Questions | Supported by |
|---|---|---|
| 51. | Do all the servers have internet access? | (*ISO/IEC 27001 Annex A.9.1.2)*<br>(*ISO/IEC 27001 Annex A.13.1)* |
| 52. | Do you have malware protection installed on the servers? | (*ISO/IEC 27001 Annex A.12.2.1)* |
| 53. | Do you have any other form of intrusion detection system available on the servers that would raise a security flag, should there be any malicious activity detected? | (*ISO/IEC 27001 Annex A.12.2.1)*<br>(*ISO/IEC 27001 Annex A.13.1)*<br>(*ISO/IEC 27001 Annex A.13.2.1)*<br>(*ISO/IEC 27001 Annex A.14.1.3)* |
| 54. | Do you have processes to periodically check if the user accounts have been properly terminated once an employee quits? It is very important in case of provisional (prv) accounts with elevated access.*)* | (*ISO/IEC 27001 Annex A.9.2.1)*<br>(*ISO/IEC 27001 Annex A.9.2.6* |
| 55. | Do the servers have any controls that block the installation of new programs on the servers (for example – Carbon Black which needs an explicit approval on the checksum value of every file being executed)? | (*ISO/IEC 27001 Annex A.12.6.2)* |
| 56. | Do you have redundant servers to ensure availability and disaster recovery? | (*ISO/IEC 27001 Annex A.17.2.1)*<br>(*ISO/IEC 27001 Annex A.13.3.1)* |
| 57. | Do you have an OS patch management system in place – installing security patches during a maintenance window to ensure the safety of the systems? | (*ISO/IEC 27001 Annex A.12.5.1)*<br>(*ISO/IEC 27001 Annex A.14.2.2)*<br>(*ISO/IEC 27001 Annex A.14.2.4)* |
| 58. | Do you have separate types of user accounts – one to access workstation and other provisional accounts to access infrastructure management resources like servers? | (*ISO/IEC 27001 Annex A.1.2.3)* |
| 59. | Is multiple-factor authentication enabled to access the servers remotely?*)* | (*ISO/IEC 27001 Annex A.9.4.2)*<br>(*ISO/IEC 27001 Annex A.9.4.3* |

**Table 19.** Framework questions about Applications **(ISO/IEC 27001, 2013)** *and (see table 14)*

| Nr. | Framework Questions | Supported by |
|---|---|---|

| | | |
|---|---|---|
| 60. | Do you have an application development team to maintain and update the in-house applications? | *(ISO/IEC 27001 Annex A.14.2.1)* |
| 61. | Do you program in-house application using "secure by design" approach? | *(ISO/IEC 27001 Annex A.14.2.1)*<br>*(ISO/IEC 27001 Annex A.14.2.5)*<br>*(ISO/IEC 27001 Annex A.14.2.6)* |
| 62. | Are these applications regularly updated considering the changing threat landscape? | *(ISO/IEC 27001 Annex A.14.1.3)*<br>*(ISO/IEC 27001 Annex A.12.2.1)*<br>*(ISO/IEC 27001 Annex A.12.1.1)* |
| 63. | Are these applications tested for any vulnerabilities from the security point of view (techniques like penetration testing, risk assessment, etc.)? | *(ISO/IEC 27001 Annex A.14.2.8)* |

**Table 20.** Framework questions about Information Management **(ISO/IEC 27001, 2013)** *and (see table 14)*

| Nr. | Framework Questions | Supported by |
|---|---|---|
| 64. | Do you have a good overview of the information assets that you possess? | *(ISO/IEC 27001 Annex A.8.1)* |
| 65. | Do you have good access control mechanisms in place so that only authorized employees can access the information? | *(ISO/IEC 27001 Annex A.8.2)* |
| 66. | Have you differentiated the information based on the criticality like terming documents are classified, confidential, private, de-classified etc. (following some model like Bell-LaPadula, Chinese wall, etc.)? | *(ISO/IEC 27001 Annex A.8.2.1)*<br>*(ISO/IEC 27001 Annex A.8.2.2)* |
| 67. | Do you have a clear desk policy – where the confidential information is not kept openly on the desk for others to be seen? | *(ISO/IEC 27001 Annex A.11.2.9)* |
| 68. | Do you have other confidentiality measures like secure printing – the print job will be finished only when the person physically shows up at the printer? | *(ISO/IEC 27001 Annex A.13.1.2)* |
| 69. | Do you use any other form of document control system like SharePoint, box, Google drive etc. for version control, collaboration or integrity check? | *(ISO/IEC 27001 Annex A.9.4.1)* |
| 70. | Do you have a system in place where the users can report any incidents related to mishandling of the information at a workplace (classified documents lying on the printer etc.) to be addressed on a case-by-case basis? | *(ISO/IEC 27001 Annex A.16.1.2)* |

## 4.5 Proposed Approach to Evaluation

As recommended in RiskM Modeling methodology principle – *Multiple phases* (Strecker, 2011) and also since the threat landscape is always evolving (Pirc, DeSanto, Gradigo, & Davison, 2015), we will follow an approach that consists of three steps. The questions asked from the rated organization will be analyzed in general and based on the threat landscape of the industry, as discussed in section 2.6. Then a SecurityScore Assessment report will be generated with three sections.

### 4.5.1 General evaluation of the information security posture

During this step, we will send the questionnaire to the organization being rated and wait for them to respond to it. Then based on the response from the questionnaire (from section 4.3), we will create an overall score (one point for each positive answer). However, there are six parts of the evaluation, i.e. Policies, Network, Storage, Servers, Applications and Information Management; as listed in table 4. An organization may be good at policies but not networks. To be explicit, we will distinguish the scoring based on critical success factors from table 4 (See report specimen on the next page). This makes the process transparent to the rated organization. Also, makes it more convenient to apply appropriate mitigation steps.

### 4.5.2 Threat landscape evaluation – sector specific (see section 2.6)

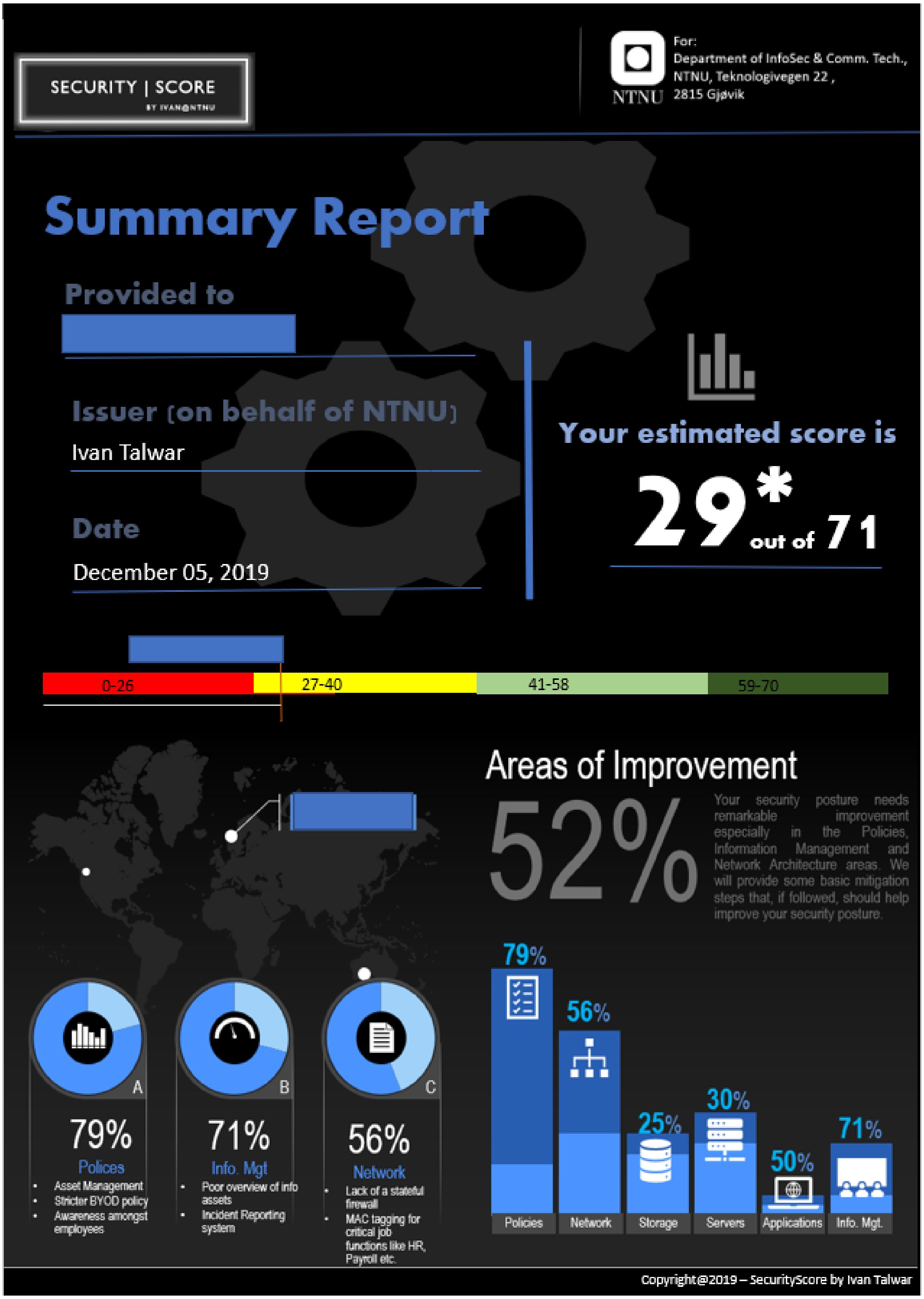
Then risks will be derived from the risk threat landscape and threat actors mentioned in section 2.6. Based on each threat actor and sector-type, a threat actor specific score will be generated. Only relevant questions to threat actor specific risks will be evaluated to generate a threat exposure score. No additional questions will be asked from the rated organization; the same data from section 4.5.1 will be used.

### 4.5.3 Recommended mitigation based on ISO 27001 recommendations)

Based on the answers from the rated organizations, some recommendations will be made based on their current security posture.

Please see below for an evaluation report specimen.

**Page 1** – Prototype *SecurityScore Assessment* Report



SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Summary Report

**Provided to**

[redacted]

**Issuer (on behalf of NTNU)**

Ivan Talwar

**Date**

December 05, 2019

**Your estimated score is**

**29* out of 71**

[redacted]

| 0-26 | 27-40 | 41-58 | 59-70 |
|---|---|---|---|

[redacted]

## Areas of Improvement

52%

Your security posture needs remarkable improvement especially in the Policies, Information Management and Network Architecture areas. We will provide some basic mitigation steps that, if followed, should help improve your security posture.

79%
Polices
- Asset Management
- Stricter BYOD policy
- Awareness amongst employees

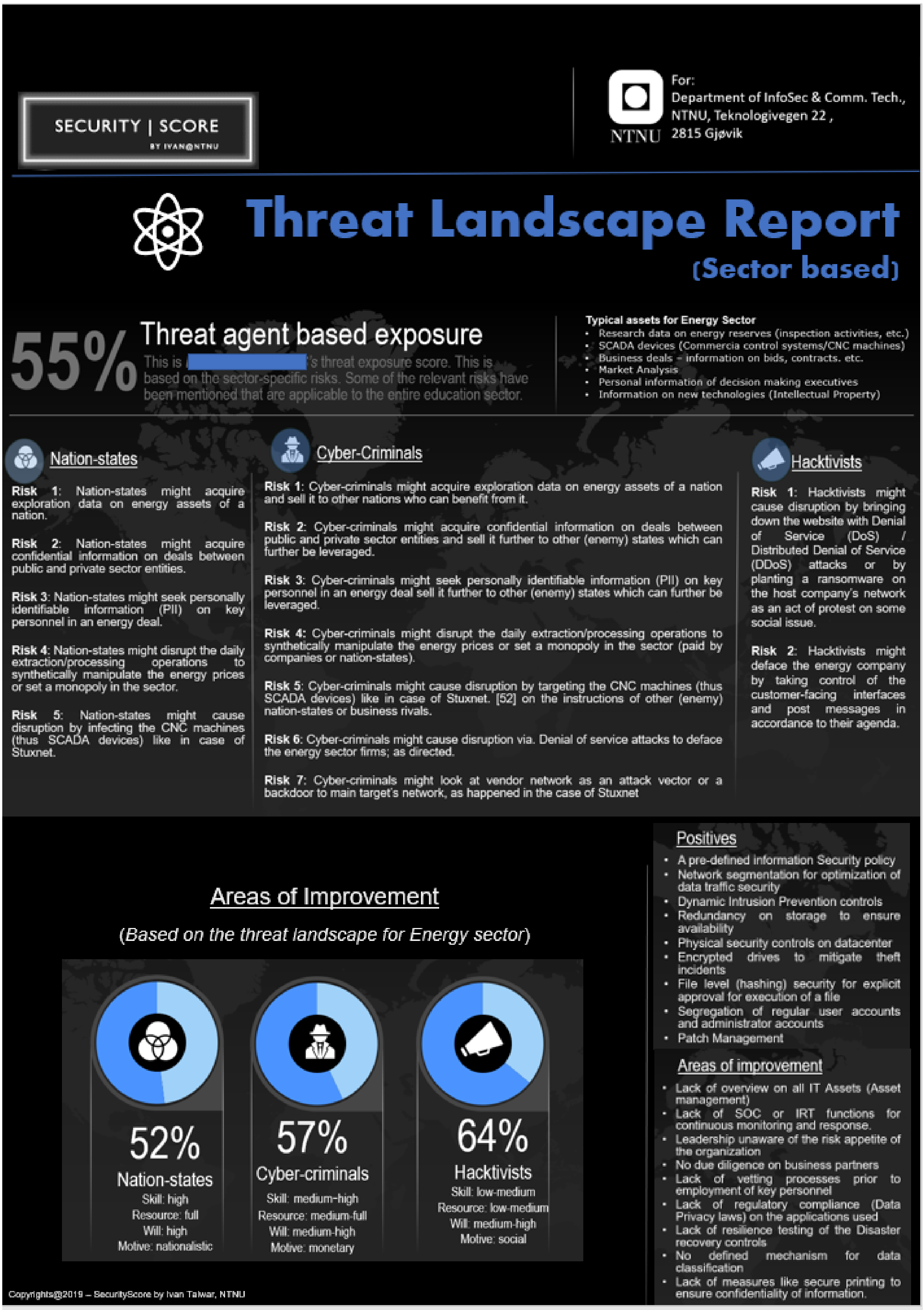
71%
Info. Mgt
- Poor overview of info assets
- Incident Reporting system

56%
Network
- Lack of a stateful firewall
- MAC tagging for critical job functions like HR, Payroll etc.

| Policies | Network | Storage | Servers | Applications | Info. Mgt. |
|---|---|---|---|---|---|
| 79% | 56% | 25% | 30% | 50% | 71% |

Copyright@2019 – SecurityScore by Ivan Talwar

**Page 2** – Prototype *SecurityScore Assessment* Report



SECURITY | SCORE
BY IVAN@NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

NTNU

# Threat Landscape Report
## (Sector based)

**55%** Threat agent based exposure

This is [redacted]'s threat exposure score. This is based on the sector-specific risks. Some of the relevant risks have been mentioned that are applicable to the entire education sector.

**Typical assets for Energy Sector**
- Research data on energy reserves (inspection activities, etc.)
- SCADA devices (Commercia control systems/CNC machines)
- Business deals – information on bids, contracts. etc.
- Market Analysis
- Personal information of decision making executives
- Information on new technologies (Intellectual Property)

### Nation-states

**Risk 1**: Nation-states might acquire exploration data on energy assets of a nation.

**Risk 2**: Nation-states might acquire confidential information on deals between public and private sector entities.

**Risk 3**: Nation-states might seek personally identifiable information (PII) on key personnel in an energy deal.

**Risk 4**: Nation-states might disrupt the daily extraction/processing operations to synthetically manipulate the energy prices or set a monopoly in the sector.

**Risk 5**: Nation-states might cause disruption by infecting the CNC machines (thus SCADA devices) like in case of Stuxnet.

### Cyber-Criminals

**Risk 1**: Cyber-criminals might acquire exploration data on energy assets of a nation and sell it to other nations who can benefit from it.

**Risk 2**: Cyber-criminals might acquire confidential information on deals between public and private sector entities and sell it further to other (enemy) states which can further be leveraged.

**Risk 3**: Cyber-criminals might seek personally identifiable information (PII) on key personnel in an energy deal sell it further to other (enemy) states which can further be leveraged.

**Risk 4**: Cyber-criminals might disrupt the daily extraction/processing operations to synthetically manipulate the energy prices or set a monopoly in the sector (paid by companies or nation-states).

**Risk 5**: Cyber-criminals might cause disruption by targeting the CNC machines (thus SCADA devices) like in case of Stuxnet. [52] on the instructions of other (enemy) nation-states or business rivals.

**Risk 6**: Cyber-criminals might cause disruption via. Denial of service attacks to deface the energy sector firms; as directed.

**Risk 7**: Cyber-criminals might look at vendor network as an attack vector or a backdoor to main target's network, as happened in the case of Stuxnet

### Hacktivists

**Risk 1**: Hacktivists might cause disruption by bringing down the website with Denial of Service (DoS) / Distributed Denial of Service (DDoS) attacks or by planting a ransomware on the host company's network as an act of protest on some social issue.

**Risk 2**: Hacktivists might deface the energy company by taking control of the customer-facing interfaces and post messages in accordance to their agenda.

### Areas of Improvement

*(Based on the threat landscape for Energy sector)*

52%
Nation-states
Skill: high
Resource: full
Will: high
Motive: nationalistic

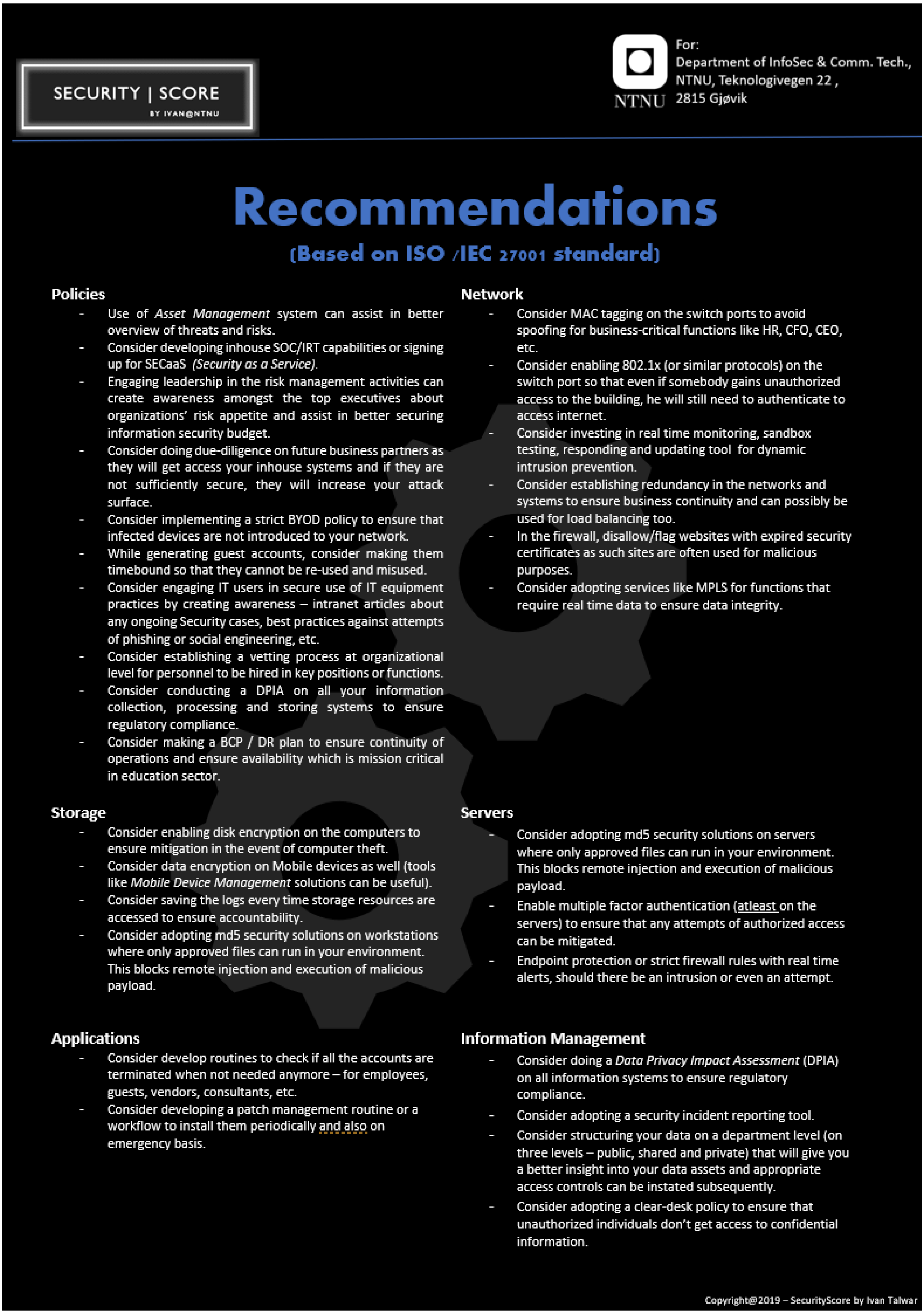
57%
Cyber-criminals
Skill: medium-high
Resource: medium-full
Will: medium-high
Motive: monetary

64%
Hacktivists
Skill: low-medium
Resource: low-medium
Will: medium-high
Motive: social

### Positives
- A pre-defined information Security policy
- Network segmentation for optimization of data traffic security
- Dynamic Intrusion Prevention controls
- Redundancy on storage to ensure availability
- Physical security controls on datacenter
- Encrypted drives to mitigate theft incidents
- File level (hashing) security for explicit approval for execution of a file
- Segregation of regular user accounts and administrator accounts
- Patch Management

### Areas of improvement
- Lack of overview on all IT Assets (Asset management)
- Lack of SOC or IRT functions for continuous monitoring and response.
- Leadership unaware of the risk appetite of the organization
- No due diligence on business partners
- Lack of vetting processes prior to employment of key personnel
- Lack of regulatory compliance (Data Privacy laws) on the applications used
- Lack of resilience testing of the Disaster recovery controls
- No defined mechanism for data classification
- Lack of measures like secure printing to ensure confidentiality of information.

*** Page 3** – General Mitigation recommendations (based on ISO/IEC 27001)



SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Recommendations

## (Based on ISO /IEC 27001 standard)

**Policies**

- Use of *Asset Management* system can assist in better overview of threats and risks.
- Consider developing inhouse SOC/IRT capabilities or signing up for SECaaS *(Security as a Service)*.
- Engaging leadership in the risk management activities can create awareness amongst the top executives about organizations' risk appetite and assist in better securing information security budget.
- Consider doing due-diligence on future business partners as they will get access your inhouse systems and if they are not sufficiently secure, they will increase your attack surface.
- Consider implementing a strict BYOD policy to ensure that infected devices are not introduced to your network.
- While generating guest accounts, consider making them timebound so that they cannot be re-used and misused.
- Consider engaging IT users in secure use of IT equipment practices by creating awareness – intranet articles about any ongoing Security cases, best practices against attempts of phishing or social engineering, etc.
- Consider establishing a vetting process at organizational level for personnel to be hired in key positions or functions.
- Consider conducting a DPIA on all your information collection, processing and storing systems to ensure regulatory compliance.
- Consider making a BCP / DR plan to ensure continuity of operations and ensure availability which is mission critical in education sector.

**Network**

- Consider MAC tagging on the switch ports to avoid spoofing for business-critical functions like HR, CFO, CEO, etc.
- Consider enabling 802.1x (or similar protocols) on the switch port so that even if somebody gains unauthorized access to the building, he will still need to authenticate to access internet.
- Consider investing in real time monitoring, sandbox testing, responding and updating tool for dynamic intrusion prevention.
- Consider establishing redundancy in the networks and systems to ensure business continuity and can possibly be used for load balancing too.
- In the firewall, disallow/flag websites with expired security certificates as such sites are often used for malicious purposes.
- Consider adopting services like MPLS for functions that require real time data to ensure data integrity.

**Storage**

- Consider enabling disk encryption on the computers to ensure mitigation in the event of computer theft.
- Consider data encryption on Mobile devices as well (tools like *Mobile Device Management* solutions can be useful).
- Consider saving the logs every time storage resources are accessed to ensure accountability.
- Consider adopting md5 security solutions on workstations where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.

**Servers**

- Consider adopting md5 security solutions on servers where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.
- Enable multiple factor authentication (atleast on the servers) to ensure that any attempts of authorized access can be mitigated.
- Endpoint protection or strict firewall rules with real time alerts, should there be an intrusion or even an attempt.

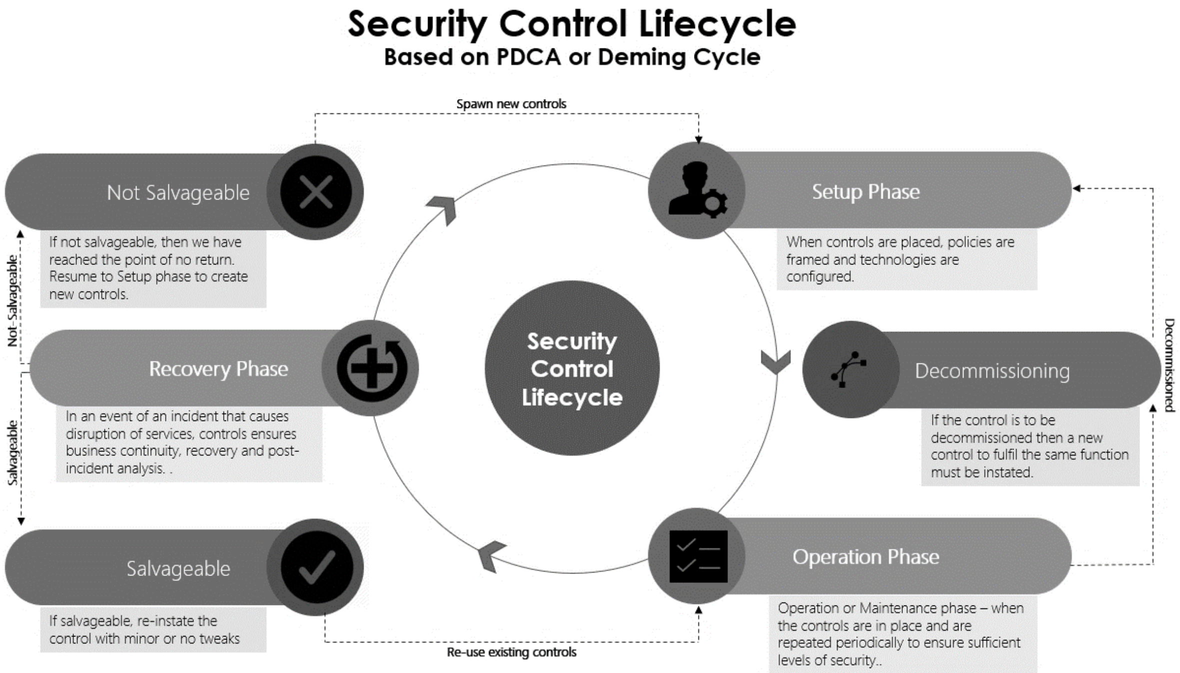
**Applications**

- Consider develop routines to check if all the accounts are terminated when not needed anymore – for employees, guests, vendors, consultants, etc.
- Consider developing a patch management routine or a workflow to install them periodically and also on emergency basis.

**Information Management**

- Consider doing a *Data Privacy Impact Assessment* (DPIA) on all information systems to ensure regulatory compliance.
- Consider adopting a security incident reporting tool.
- Consider structuring your data on a department level (on three levels – public, shared and private) that will give you a better insight into your data assets and appropriate access controls can be instated subsequently.
- Consider adopting a clear-desk policy to ensure that unauthorized individuals don't get access to confidential information.

Additionally, the controls in the proposed *SecurityScore Assessment* model can be periodically checked and either be revised or de-commissioned based on the *Plan Do Check Act (PDCA )or Deming cycle* (Meng, 2013).


Security Control Lifecycle

Based on PDCA or Deming Cycle

If not salvageable, then we have reached the point of no return. Resume to Setup phase to create new controls.

When controls are placed, policies are framed and technologies are configured.

In an event of an incident that causes disruption of services, controls ensures business continuity, recovery and post-incident analysis. .

If the control is to be decommissioned then a new control to fulfil the same function must be instated.

If salvageable, re-instate the control with minor or no tweaks

Operation or Maintenance phase – when the controls are in place and are repeated periodically to ensure sufficient levels of security..

**Figure 4.2.** Proposed security Control Lifecycle based on the Deming Cycle **(Meng, 2013)**

# 5 Conclusions

Four organizations participated in the risk rating evaluation survey. The organizations belonged to *education, energy and maritime* sector. The maritime firm scored the best while the energy sector firm saw the biggest room for improvement. *3 out of 4 firms* showed the biggest scope of improvement in the areas of *policies* and *information management*. When the evaluation reports were sent to them, an explanation of scoring was also attached to the email to make it understandable to them how the scoring took place. Also, the feedback was sought from them to further improve the model.

## 5.1 Solutions to our problem questions

- *What are the existing security rating methods available today to quantify information security risks (applicable to our scenarios), and what are their pros and cons?*
  There are multiple security rating methods available – open source like CVSS 3.0 and OWASP Risk Rating methodology, but they are more inclined towards quantifying software vulnerabilities.
  There are multiple commercial solutions available too, but they are quite opaque in their methodologies.

- *Can an efficient and scientifically repeatable framework be developed by learning from these methods and rating systems?*
  it is hard to recreate the same results by the rated organization itself or by another firm providing similar solutions for that matter since the modus operandi differs in all cases.

- *Can the framework cover all the key components of an IT Infrastructure and set of policies that reflect on the Information Security posture of an organisation?*
  Open source solutions cover only software vulnerability factors, and the commercial solution does not provide information publicly on what factors do they consider during the evaluation process. Therefore, there is no way to verify if these solutions cover all factors of an IT Infrastructures and all processes around it.

- *Can this new point-based framework be developed in such a way that it is easy to use, transparent, and covers most of the key components and aspects of an IT eco-system in a checklist form?*
  A new point-based system called *SecurityScore assessment* has been developed that measures the critical success factors for assessing security performance. It is easy to use, and anybody in an IT department or IT support role can answer this questionnaire without specialized knowledge into information security domain.

  Post-evaluation, *Education_1 Corp*. and *Education_2 Corp.* remarked that the model is very easy to understand and is very helpful in understanding their security posture. This will add a great value to their organizations.

- *Can this framework provide a sector-specific risk assessment?*

SecurityScore Assessment quantifies both general security posture as well as sector-specific performance.

- *Can this framework solve any other issues with the findings of the research?* SecurityScore Assessment can potentially be used as a universal security scoring system (on the lines of credit score). See Section 5.3 for a few more applications.

  *Based on our scenario 1* – While sending a bid for a contract, the SecurityScore can be attached with the bid. A certain percentage of weightage should be given to SecurityScore results since the client will share their systems with the vendor. By choosing a specific vendor, the client adds the attack surface of the vendor to their own.

  *Based on our scenario 2* – During mergers and acquisitions, the parent company can run this check on their own infrastructure and policies. The results can be compared with those of the sister company being merged or acquired. Whosoever has a better security posture; their IT policies and practices should be used as a template for the other to use. Since they both will use a standard procedure, the results will be comparable as is otherwise when due diligence is performed by different organizations separately in different and non-comparable ways.

## 5.2 Observations during the evaluation process

- When I approached the participating organizations, they were happy to share the state of their current security posture by answering the questionnaire and receive a free copy of the evaluation. It shows that some organizations may be aware of the consequences of information security, but due to lack of resources or attention from the top management, they cannot spend time and resources to do better with risk management.
- The questionnaire was easy to understand and did not receive any queries about the ambiguity of the questions. It shows that the questionnaire framework was easily understood which one of our aims was.
- The modus operandi of scoring is very straight forward and was explained to the participating firms in the report email, i.e. one point for each applicable question. And relevant risk related questions based on the sector to present a sector specific score. It is easy to use this framework as a benchmark and keep updating the points as and when new measures are taken. This process is repeatable too.
- The entire evaluation process satisfied the principles of *RiskM model* as mention in Table 7. The evaluation report sent to the rated organization is easy to read and easily be understood by a novice. It provides a basis for decision making on risks (principle 1) by providing an organizations' security posture (principle 2), measuring practices and giving recommendation to multiple levels with an organization (principle 3), provides quantitative values (in the form of SecurityScore) and qualitative recommendation to improve the score (principle 4), the evaluation method is verified against *ISO 27001* standard (principle 5) and perform in multiple phases (evaluation and improvements in the model itself based on principle 6).
- Since it is easy to use and effective in measuring the critical success factors of security performance (table 4), it can easily be used across sectors to at least

quantify the general security posture of an organization. If made available publicly and freely, it can be used by organizations that do not have the means to avail such services. This increases the potential of this model to be used as a standard model in the sector.

## 5.3 Miscellaneous applications of SecurityScore Assessment

- It can be used as a benchmarking tool by the organization to see and follow their progress towards their information security goals.
- It can be used as a universal scale to measure information security preparedness by the Insurance sector. Based on this score and the size of the organization, the annual premium can be decided.

# 6 Limitations and scope of future research

## 6.1 Limitations realized during the research

- The short duration of the research is the biggest road-block to further elaborating the framework.
- The evaluation process is manual, and the report must be generated manually, which takes time and effort.
- Since this is an upcoming issue, there is not elaborate literature available for our specific problems.
- It can be challenging to get organizations onboard the research as they do not wish to reveal their IT practices. Section 3 in the *SecurityScore Assessment* report is to compensate for their efforts by providing them with pin-pointed recommendations based on industry standards.

## 6.2 Scope of further research

- The future researchers can dig deeper and probe about the cloud-based infrastructure. Since the public cloud provider has a common risk portfolio that all the tenants share, some mechanism can be used to derive that information from central databases like *Cloud Alliance Star Registry*.
- I managed to gather data on 4 organization, but if more data is collected over a period of time, it can be used to benchmark industries. Then mean scores, standard deviation, skewness of the data can be used to even validate the effectiveness of certain questions and general trends in the industry.
- The evaluation and reporting process can be automated to save time and effort. The solution can then be put on a website where organizations can freely use the solution.

# 7 Bibliography

**Interviews**

Bøe, L. (2018, November 19). Experience of AGR Merger with Oceaneering. (I. Talwar, Interviewer) – *See Appendix 1*

Felde, M. (2018, 08 11). Senior Manager, Risk Advisory. Questions on Mergers and Acquisitions. (I. Talwar, Interviewer) – *See Appendix 2*

Ng, K. (2018, 12 26). Information on the bidding process (Client-Vendor dealing). (I. Talwar, Interviewer) - *See Appendix 3*

Timmerman, T. (2018, 11 07). Senior Manager (Cyber Risk, KPMG).Due Dilligence process in Mergers and Acquisitions. (I. Talwar, Interviewer) - *See Appendix 4*

**Literature sources**

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy006,, 4*(1), 1-15. doi:https://doi.org/10.1093/cybsec/tyy006

Alaranta, M., & Mathiassen, L. (2014, 01 01). Managing Risks: Post-Merger Integration of Information Systems. *16*(1), ss. 30-40. doi:10.1109/MITP.2013.64

Aleksandrova, S., Aleksandrov, M., & Vasiliev, V. (2018). Business Continuity Management System. *2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)* (pp. 14-17). St. Petersburg, Russia: IEEE. doi:10.1109/ITMQIS.2018.8525111

Angraini, Megawati, & Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. *The 6th International Conference on Cyber and IT Service Management (CITSM 2018)* (s. 4). Medan: IEEE. doi:10.1109/CITSM.2018.8674294

Angraini, N., Megawati, N., & Haris, L. (n.d.). Risk Assessment on Information Asset an academic. *The 6th International Conference on Cyber and IT Service Management (CITSM 2018). 6th.* Parapat, Indonesia: IEEE. doi:10.1109/CITSM.2018.8674294

Anthony for KPMG, S. (2015). Data Protection, Privacy and Cyber Security. *ISACA Kenya Annual Conference - Secure Kenya II* (s. 45). Mombasa: ISACA. Hentet 11 21, 2019 fra http://isaca.or.ke/downloads/Data-Protection-Privacy-and-Cybersecurity.pdf

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber Security Concerns in E-Learning Education (ISBN: 978-84-617-2484-0 ). *Proceedings of ICERI2014 Conference* (ss. 0729-0734). Seville: The Open University. Hentet 11 02, 2019 fra http://oro.open.ac.uk/id/eprint/59105

Banerjee, A., Venkatasubramanian, K., Mukherjee, T., & Gupta, S. (2012, January). Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems. *Proceedings of the IEEE, 100*(1), ss. 283-299. doi:10.1109/JPROC.2011.2165689

Banham 2, R. (2017, June). Investing in the Insurtech Toolbox. *Risk Management, 64*(6), 12-14. Hentet 10 02, 2019 fra https://search.proquest.com/docview/1912096332?accountid=12870

Banham, R. (2017, November). CYBER SCOREKEEPERS. *Risk Management, 64*(10), 26-29. Hentet 10 20, 2019 fra https://search.proquest.com/docview/1965148282?accountid=12870

Bartlett, M. (2014, January 27). How Baxter CU Prevents Internal Fraud With Careful Hiring, Training Practices: Strong Due Diligence Before Bringing New Employees On Board, Rigorous Onboarding Process After Is Key. *Credit Union Journal, 18*(4), 12. Hentet 10 11, 2019 fra https://search.proquest.com/docview/1491853695?accountid=12870

Bartosz, B., Brzoza-Woch, R., Bubak, M., Kasztelnik, M., Kwolek, B., Nawrocki, P., . . . Zielinski, K. (2018, February). Holistic approach to management of IT infrastructure for environmental monitoring and decision support systems with urgent computing capabilities. *Future Generation Computer Systems, 79*(1), 128-143. doi:https://doi.org/10.1016/j.future.2016.08.007

Baskerville, R. (1993, December). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375-414. doi:10.1145/162124.162127

Beale, I. (2017, July 19). Volume 11 Number 2. (H. S. LLP, Red.) *Best practice vendor risk management in today's interconnected world, 11*(2), 151-163. Hentet 08 02, 2019 fra

http://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=126935164&site=ehost-live

Beaver, K. (2014, March). The Target Breach - Can it be prevented? *Security Technology Executive, 24*(1), 12,50. Hentet 10 20, 2019 fra https://search.proquest.com/docview/1524987943?accountid=12870

Bernik, I., & Prislan, K. (2016, September 21). *Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation.* West Virginia University, UNITED STATES. West Virginia: PLoS ONE. doi:10.1371/journal.pone.0163050

Bhoola, V., Hiremath, S., & Mallik, D. (2014). AN ASSESSMENT OF RISK RESPONSE STRATEGIES PRACTICED IN SOFTWARE PROJECTS. *Australasian Journal of Information Systems, 18*(3), 161-191. doi:10.3127/ajis.v18i3.923

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL. (2019). *THE GUIDELINES ON THE GUIDELINES ONBOARD SHIPS.* Washington D.C: BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL. Hentet 10 03, 2019 fra https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

Bruijne, M., Eeten, M., Gañán, C. H., & Pieters, W. (2017, July 01). Towards a new cyber threat actor typology - A hybrid method for the NCSC cyber security assessment. Delft, South Holland, Netherlands: National Cyber Security Centre (a division of Ministry of Safety and Justice, Netherlands). Hentet 11 01, 2019 fra https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf

Canadian Centre for Cyber Security. (2018, 12 06). *An introduction to the Cyber threat environment - Cyber Threat and Cyber Threat Actors*. Hentet fra https://cyber.gc.ca/: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

Chapman, D. (2019). *How safe is your data? Cyber-security in higher education.* Joint Information Systems Committee, Security Operations Centre. Oxford: HEPI. Hentet 11 02, 2019 fra https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf

Chapman, M. (2014). *Target: Data breach caught up to 70M customers.* Spartanburg, S.C.: Halifax Media Group. Hentet 10 10, 2019 fra https://search.proquest.com/docview/1476830117?accountid=12870

Cloud Security Alliance. (2017). *CSA STAR Registry - Security Trust Assurance and Risk Registry*. Retrieved 09 10, 2019, from cloudsecurityalliance.org: https://cloudsecurityalliance.org/star/registry/

Courtney Jr. , R. H. (1977). Security risk assessment in electronic data processing systems. *AFIPS '77 Proceedings of the June 13-16, 1977, national computer conference* (ss. 97-104). Dallas, Texas: ACM. doi:10.1145/1499402.1499424

D'Arcy, J., Hovav, A., & Galletta, D. . (2009, March). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98,155.157. doi:10.1287/isre.1070.0160

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical Benefits of Training to Phishing Susceptibility. In W. P. United States Military Academy, *Information Security and Privacy Research - SEC 2012* (Vol. 376, pp. 457-464). New York, USA: Springer, Berlin, Heidelberg. doi:https://doi.org/10.1007/978-3-642-30436-1_37

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers and Security, 25*(1), 55-63. doi:https://doi.org/10.1016/j.cose.2005.09.009

Dulaney, E., & Stinson, K. (2011). *CompTIA Security+ Deluxe Study Guide (PRINT ISBN - 9781118014745).* Hoboken, NJ: John Wiley & Sons, Incorporated.

Enaw, E. E., & Check, N. (2018). Information Systems Security Audits in Cameroon's Public Administration. *ICEGOV '18 Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance* (pp. 312-317). Galway, Ireland: ACM, New York, USA. doi:10.1145/3209415.3209425

ENISA 2. (2011). *ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARTIME SECTOR.* Athens: ENISA. Hentet 10 02, 2019 from https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

ENISA. (2019). *ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends.* Athens: ENISA. doi:10.2824/622757

ENISA 4. (2018). *ICT security certification opportunities in the healthcare sector (ISBN - 978-92-9204-276-9).* Attiki: ENISA. doi:10.2824/939028

Fang, B. (2018). In C. E. CorporationBeijingChina, *Cyberspace Sovereignty* (pp. 243-320). Beijing, China: Springer, Singapore. doi:https://doi.org/10.1007/978-981-13-0320-3_8

Fangyong, H., Hongjun, H., & Nong, X. (2009). Hash Tree Based Integrity Protection Appropriate for Disk. *2009 WASE International Conference on Information Engineering* (ss. 242-245). Taiyuan, Chanxi, China: IEEE. doi:10.1109/ICIE.2009.178

Fanimokun, A. O. (2012). The use of NDAs in the IT service sector. In B. R. Florida Atlantic University, *Service Business* (pp. 123-136). Boca Raton: Springer-Verlag. doi:https://doi.org/10.1007/s11628-009-0076-4

Felde, M. (2018, 08 11). Senior Manager, Risk Advisory.

First.org. (2005, 02 23). *Introduction to CVSS*. Retrieved from first.org: https://www.first.org/cvss/v1/intro

first.org. (2019). *Common Vulnerability Scoring System v3.1: Specification Document.* Retrieved from first.org: https://www.first.org/cvss/v3.1/specification-document

First.org. (2019, 06 01). *Common Vulnerability Scoring System version 3.1: Specification Document.* Retrieved 03 02, 2019, from www.first.org: https://www.first.org/cvss/specification-document

Firstenberg, M. H. (2016). Cyber Security: How much is enough? *Sans Cyber Security Summit.* Sans.org / Winterfall. Retrieved from https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493604914.pdf

FrSecure. (2019). *FISASCORE - Fiducial Information Security Assessment Score*. Retrieved from https://frsecure.com: https://frsecure.com/services/fiducial-information-security-risk-assessment-score-fisascore/

GDPR Peras, D. (2018). Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses. *Central European Conference on Information and Intelligent Systems* (ss. 113-121). Varazdin: Faculty of Organization and Informatics Varazdin. Hentet 10 02, 2019 fra https://search.proquest.com/docview/2125639461?accountid=12870

Gelbstein, E. (2013). Quantifying Information Risk and Security. *ISACA Journal, 4*, 33-38. Retrieved from https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Quantifying-Information-Risk-and-Security.aspx

Gerber, M., & Solms, R. (2005, 02). Management of risk in the information age. *Computers & Security, 24*(1), 16-30. doi:https://doi.org/10.1016/j.cose.2004.11.002

Gleich , R., Kierans, G., & Hasselbach, T. (2010). *Value in Due Diligence : Contemporary Strategies for Merger and Acquisition Success.* Farnham, Surrey [U.K.]. Hentet 10 21, 2019 fra http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=389870&site=ehost-live.

Govindaraju, R., Akbar, R., & Suryadi, K. (2018, 06). IT Infrastructure Transformation and its Impact on IT Capabilities in the Cloud Computing Context. *International Journal on Electrical Engineering and Informatics, 10*(2), 395-405. doi:http://dx.doi.org/10.15676/ijeei.2018.10.2.14

Greitzer, F. L., Purl, J., Leong, Y. M., & Sticha, P. J. (2019, 06 01). Positioning Your Organization to Respond to Insider Threats. *IEEE Engineering Management Review, 47*(2), 75-83. doi:10.1109/EMR.2019.2914612

Guarro, S. B. (1987, December). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers & Security, 6*(6), 493-504. doi:https://doi.org/10.1016/0167-4048(87)90030-7

Higgins, J. (2017). *U.S. Chamber issues principles for Ôfair and accurate' cybersecurity ratings.* Arlington: ProQuest. Hentet 10 02, 2019 fra https://search.proquest.com/docview/1911558501?accountid=12870

Hoffman, L. J., Michelman, E. H., & Clements, D. (1978, 01 01). SECURATE-Security evaluation and analysis using fuzzy metrics*. (ss. 531-540). Arlington: Sematics Scholar. Hentet 09 21, 2019 fra https://pdfs.semanticscholar.org/e9f3/02da3bec9a9477932cfeb57e6d82ab3b42e7.pdf

Hong, K.-S., Chi, Y.-P., Chao, L., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248. doi:https://doi.org/10.1108/09685220310500153

Hooper, V., & McKissack, J. (2016, November). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. doi:https://doi.org/10.1016/j.bushor.2016.07.004

Hsu, S. (2018). IT Infrastructure (eISBN: 9780191839023). I S. Hsu, *A Dictionary of Business and Management in China* (Fifth. utg., s. 93). Oxford: Oxford University Press. doi:10.1093/acref/9780191839023.001.0001

*IDC Survey: Downtime Costs Large Companies Billions*. (2015). Retrieved from http://www.devopsdigest.com: http://www.devopsdigest.com/idc-survey-appdynamics-devops-application-performance

Instablogs. (2010, April 01). Windows 7 is impossible to hack if Administrator Rights are used properly. *Computers--Internet*, s. 1. Hentet 10 01, 2019 fra https://search.proquest.com/docview/189741902?accountid=12870

Isabella, S. (2008, September). Secure printing. *Datenschutz und Datensicherheit - DuD, 32*(9), 593-596. doi:https://doi.org/10.1007/s11623-008-0141-5

ISO/IEC 17799. (2005, 06 15). ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management. *Information technology — Security techniques — Code of practice for information security management*. Geneva, Geneva, Switzerland: NEK ISO/IEC. Hentet 08 20, 2019

ISO/IEC 27001. (2013, 09 25). ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements. *Information technology -- Security techniques -- Information security management systems -- Requirements*. Geneva, Switzerland, unknown, unknown: NEK ISO/IEC.

John, J., Sural, S., & Gupta, A. (2017, June 27). Attribute-based access control management for multicloud collaboration. *Concurrency and Computation, 29*(19), 14. doi:https://doi.org/10.1002/cpe.4199

Johnson, B. R., Onwuegbuzie, A. J., & Turner, L. A. (2007, April 01). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research, 1*(2), 112-133. doi:https://doi.org/10.1177/1558689806298224

Koivunen, E. (2010). "Why Wasn't I Notified?": Information Security Incident Reporting Demystified. *Nordic Conference on Secure IT Systems, Part of the Lecture Notes in Computer Science book series (LNCS, volume 7127)*, 55-70. doi:https://doi.org/10.1007/978-3-642-27937-9_5

Korolov, M. (2017, December 06). Supply chain attacks: be wary of third-party providers. *Computerworld Hong Kong; Newton*, s. 5. Hentet 10 02, 2019 fra https://search.proquest.com/docview/1973229926?accountid=12870

KPMG. (2014). *Cyber Security: It's not just about technology.* Delaware, US: KPMG. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf

KPMG. (2018). *Vendor security risk management*. Retrieved from home.kpmg: https://home.kpmg/content/dam/kpmg/ca/pdf/2017/10/vendor-security-risk-management-kpmg-canada.pdf

Larsen, L. B. (2018, 11 19). CEO, Marin IT (DOF Subsea). (I. Talwar, Interviewer)

Leedy, P. D., & Ormod, J. E. (2019). *Practical Research - Planning and Design - Eleventh edition (Global Edition).* Essex, England: Peason Education Limited. Retrieved 10 16, 2019

Li, Y., Cui, W., Li, D., & Zhang, R. (2011). Research based on OSI model. *2011 IEEE 3rd International Conference on Communication Software and Networks* (pp. 554-557). Xi'an, China: IEEE. doi:10.1109/ICCSN.2011.6014631

Liang, X., & Xiao, Y. (2013). Game Theory for Network Security. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013*, 472-486. doi:10.1109/SURV.2012.062612.00056

Lidster, W. W., & Rahman, S. (2018). Obstacles to Implementation of Information Security Governance. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th* (pp. 1826-1831). New York, USA: IEEE. doi:10.1109/TrustCom/BigDataSE.2018.00276

Liu, R., & Lee, J. (2012). IT incident management by analyzing incident relations. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 7636*, ss. 631-638. Berlin: Scopus (Elsevier B.V). doi:10.1007/978-3-642-34321-6-49

Loots, M. (2001). Importance of a security policy. *South African Journal of Information Management, 3*(2), 22. Hentet 10 30, 2019 fra https://pdfs.semanticscholar.org/63f4/8a40f006c8e0c1de52903649217e589b89db.pdf

Lynett, M. (2015). *A History of Information Security From Past to Present.* Ontario, Canada: MES. Retrieved from https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present

Mahfuth, A., Yussof, S., Baker, A. B., & Ali, N. . (2017). A Systematic Literature Review: Information Security. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS).* Langkawi, Malaysia: IEEE. doi:10.1109/ICRIIS.2017.8002442

Meirkhanova, A. (2019). *Information security expertise and oversight among Norwegian boards of directors.* Norwegian University of Science and Technology (NTNU), Department of Information Security and Communication Technology. Gjøvik: Norwegian University of Science and Technology (NTNU). Hentet 11 20, 2019 fra http://hdl.handle.net/11250/2617755

Meng, M. (2013). The research and application of the risk evaluation and management of information security based on AHP method and PDCA method. *2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering.* Xi'an, China: IEEE. doi:10.1109/ICIII.2013.6703597

More, J., Stieber, A., & Liu, C. (2016). Chapter 1.2 - Tier 1—Patch Management. I J. More, A. J. Stieber, & C. Liu, *Breaking into Information Security* (ss. 42-44). Amsterdam: Elsevier B.V. doi:https://doi.org/10.1016/B978-0-12-800783-9.00006-9

Mukhopadhyay, A., Das, S., Sadhukhan, S. K., & Saha, D. (2013). Vulnerable path determination in mobile ad-hoc networks using Markov Model. *Proceedings of the 19th Conference Amercias Conference on Information Systems (AMCIS).* Chicago, illinois: Association for Information systems. Hentet 10 02, 2019 fra https://pdfs.semanticscholar.org/49a7/b93a83bfcf302e952c1f4ecf11a3a8dec820.pdf

Mukhopadhyay1, A., Chatterjee2, S., Bagchi3, K. K., Kirs, P. J., & Shukla, G. K. (2019, 10). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers, 21*(5), 997-1018. doi:https://doi.org/10.1007/s10796-017-9808-5

Nieles, Michael; Dempsey, Kelley; Pillitteri, Victoria Yan;. (2017, June). An Introduction to Information Security. *NIST Special Publication 800-12*, on Page 2 (last paragraph). doi:https://doi.org/10.6028/NIST.SP.800-12r1

NIST 2. (2005, 03). Minimum Security Requirements for Federal. *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*, 11. Hentet 10 02, 2019 fra https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

NIST. (2012, 01 01). COMPUTER SECURITY RESOURCE CENTER (CSRC). Gaithersburg, Maryland, USA: National Institute of Standards and Technology. Hentet 10 02, 2019 fra https://csrc.nist.gov/glossary/term/threat

NIST. (2016). *Vulnerability Metrics*. Hentet fra https://nvd.nist.gov/: https://nvd.nist.gov/vuln-metrics/cvss

NIST 3. (2019, 01 01). NATIONAL VULNERABILITY DATABASE. Gaithersberg, Maryland, USA: NIST. Hentet 10 02, 2019 fra https://nvd.nist.gov/

O'Hara, B. T., & Malisow, B. (2017). Data Classification (Chapter 3). I B. T. O'Hara, & B. Malisow, *Certified Cloud Security Professional* (ss. 43-66). Indianapolis, Indiana, USA: John Wiley & Sons, Inc. doi:10.1002/9781119419372.ch3

Olalere, M., Abdullah, M., Mahmod, R., & Abdullah, A. (2016). Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication. *International Journal of Computer Networks and Communications Security, 4*(1), 21-32. Hentet 10 22, 2019 fra https://search.proquest.com/docview/1862879562?accountid=12870

OWASP. (2019, June 27). *OWASP Risk Rating Methodology.* Retrieved from owasp.org: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Ozier, W. (1989, 10). Risk quantification problems and Bayesian decision support system solutions. *Information Age, 11*(4), 229-234. Hentet 10 02, 2019 fra https://dl.acm.org/citation.cfm?id=69141

Park, J., Noh, J., Kim, M., & Kang, B. (2017, June 01). Invi-server: Reducing the attack surfaces by making protected server invisible on networks. *Computers & Security, 67*, ss. 89-106. doi:https://doi.org/10.1016/j.cose.2017.02.012

Perpetus , J. H., & Joël , T. H. (2015). Measuring Information Security: Understanding And Selecting Appropriate Metrics. *International Journal of Computer Science and Security (IJCSS), 9*(2), 108-112.

Pirc, J., DeSanto, D., Gradigo, W., & Davison, I. (2015). *Threat Forecasting - Leveraging Big Data for Predictive Analysis (ISBN - 978-0-12-800006-9).* Amsterdam: Elsevier Inc. doi:https://doi.org/10.1016/C2013-0-13973-6

Plachkinova, M., & Maurer, C. (2018, Winter). Teaching case: Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-19. Hentet 09 20, 2019 fra https://search.proquest.com/docview/2018608701?accountid=12870

Professional Services Close - Up. (2018). *Opus & Ponemon Institute Highlights Results of Third-Party Data Risk Study.* Jacksonville: Close-up and Media Inc. Hentet 10 18, 2019 fra https://search.proquest.com/docview/2139018489?accountid=12870

Rainer Jr., R., Snyder, C., & Carr, H. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems, 8*(1), 129-147. doi:https://doi.org/10.1080/07421222.1991.11517914

Rieb, A., Gurschler, T., & Lechner, U. (2017, October 11). A Gamified Approach to Explore Techniques of Neutralization of Threat Actors in Cybercrime. *APF 2017: Privacy Technologies and Policy*, 87-103. doi:https://doi.org/10.1007/978-3-319-67280-9_5

Rifkin, G. (1989, 10 18). The 1980s: A Retrospective. *Computerworld, 23*(51), s. 55. Hentet 10 01, 2019 fra https://search.proquest.com/docview/215979016?accountid=12870

Ruohonen, J. (2019, July). A look at the time delays in CVSS vulnerability scoring. *Applied Computing and Informatics, 15*(2), 129-135. doi:https://doi.org/10.1016/j.aci.2017.12.002

Schneider, F. (2018). Privacy and Security Putting Trust in Security Engineering: Proposing a stronger foundation for an engineering discipline to support the design of secure systems. *Communications of the ACM, 61*(5), 37-39. doi:10.1145/3199601

Science Direct. (2019, 00 00). Vulnerability Database. Amsterdam, Amsterdam, Netherlands. doi:https://www.sciencedirect.com/topics/computer-science/vulnerability-database

Sechel, S. (2017, 01 01). Web Applications Vulnerability Management using a Quantitative Stochastic Risk Modeling Method. *Informatică economică, 21*(3), 16-30. doi:10.12948/issn14531305/21.3.2017.02

Security Scorecard Inc. (2017). *Key Industry Findings & Insights.* New York, USA: Security Scorecard Inc. Retrieved 04 20, 2019, from https://explore.securityscorecard.com/rs/797-BFK-857/images/SecurityScorecard-2017-govt-cybersecurity-report.pdf

Security Scorecard Inc. (2017). *Scoring Methodology.* New York, USA: Security Scorecard Inc. Retrieved 03 02, 2019, from https://explore.securityscorecard.com/rs/797-BFK-857/images/Scoring%20Methodology.pdf

Seebruck, R., & . (2015, September). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36-45. doi:https://doi.org/10.1016/j.diin.2015.07.002

Shabtai, A., & Elovici, Y. (2014). POSTER: Misuseablity Analysis for IT Infrastructure. *CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1496-1498 ). Scottsdale, Arizona: ACM. doi:doi>10.1145/2660267.2662385

Shepperd, M. (2015, 02 01). How Do I Know Whether to Trust a Research Result? *IEEE Software, 32*(1), 106-109. doi:10.1109/MS.2015.8

Sidhpurwala, H. (2013). *A Brief History of Cryptography.* Pune, India: Redhat. Retrieved from https://access.redhat.com/blogs/766093/posts/1976023

Smith, E., & Eloff, J. (2002, June). A Prototype for Assessing Information Technology Risks in Health Care. *Computers & Security, 21*(3), 266-284. doi:https://doi.org/10.1016/S0167-4048(02)00313-9

Snedaker, S., & Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals (ISBN - 978-0-12-410526-3).* Amsterdam: Elsevier Inc. doi:https://doi.org/10.1016/C2012-0-06206-0

Spanos, , G., & Angelis, L. (2013). WIVSS: a new methodology for scoring information systems vulnerabilities. *In Proceedings of the 17th Panhellenic Conference on Informatics (PCI '13)* (pp. 83-90). NY, USA: ACM. doi:http://dx.doi.org/10.1145/2491845.2491871

Stephenson, P. (2012, February 23). Enterprise whole disk encryption done right. *Computers--Computer Security, Criminology And Law Enforcement--Security,* *Criminology And Law Enforcement, 23*(2), s. 56. Hentet 10 02, 2019 fra https://search.proquest.com/docview/922767550?accountid=12870

Strecker, S. (2011, September). RiskM: A multi-perspective modeling method for IT risk assessment. *Information Systems Frontiers, 13*(4), 595-611. doi:https://doi.org/10.1007/s10796-010-9235-3

Takamura, E., Mangum, K., Wasiak, F., & Gomez-Rosa , C. (2015). Information Security Considerations for Protecting. *2015 IEEE Aerospace Conference* (pp. 1-14). Big Sky, Montana, USA: IEEE. doi:10.1109/AERO.2015.7119207

Taylor, N., Olstam, J., Nernhardsson, V., & Nitsche, P. (2017). Modelling delay saving through pro-active incident management techniques. *European Transport Research Review*, 17. doi:https://doi.org/10.1007/s12544-017-0265-5

Tudor, J. (2000). *Information Security Architecture - ISBN - 0-8493-9988-2* (1. utg.). Auerbach Publications / CRC Press. Hentet 10 03, 2019

US Chamber of Commerce. (2017). *Principles for Fair and Accurate Security Ratings.* Washing DC: US Chamber of Commerce. Hentet 10 28, 2019 fra https://www.uschamber.com/sites/default/files/principles_for_fair_and_accurate_security_ratings.finallist_1.pdf

Weishäup, E., Yasasin, E., & Schryen, G. (2018, August). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security, 77*, 807-823. doi:https://doi.org/10.1016/j.cose.2018.02.001

Westerman, G., & Hunter, R. (2007). IT risk; turning business threats into competitive advantage. *Reference and Research Book News, 22*(4), 221. Hentet 11 01, 2019 fra https://search.proquest.com/docview/199713921?accountid=12870

Wood, C. (2016, February 19). Hospital's Ransomware Attack Highlights Importance of Strong Endpoint Protection (ISBN -10439668). *Government Technology; Folsom*, s. 3. Hentet 10 17, 2019 fra https://search.proquest.com/docview/1767076576?accountid=12870

Xia, M., Guo, M., Wang, H., & Wang, J. A. (2009). Security Metrics for Software Systems. In ACM (Ed.), *ACM-SE 47 Proceedings of the 47th Annual Southeast Regional Conference* (p. 6). Clemson, South Carolina: ACM. doi:10.1145/1566445.1566509

Tuttle, H. (2018). 2018 CYBERRISK LANDSCAPE. *Risk Management, 65*(1), 18-21,24-25. Retrieved from https://search.proquest.com/docview/2010646013?accountid=12870

# Image sources

| **Figure** | **Source** |
|---|---|
| Figure 2.1 | https://www.first.org/cvss/v3.1/specification-document |
| Figure 2.2 | https://explore.securityscorecard.com/rs/797-BFK-857/images/Scoring%20Methodology.pdf |
| Figure 2.4 | http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf |
| Figure 2.5 | https://doi.org/10.1007/s10796-010-9235-3 |
| Figure 2.6 | https://assets.kpmg/content/dam/kpmg/pdf/2016/06/cyber-maturity-assessment-service-sheet.pdf |
| Figure 4.2 | https://en.wikipedia.org/wiki/PDCA |

# Appendices

**Appendix 1 – Interview questions** *(Lillian Bøe, Marin IT AS)*

**Appendix 2 – Interview questions** *(Magnus Felde, Deloitte)*

**Appendix 3 – Interview questions** *(Kimberly Ng, Halfwave AS)*

**Appendix 4 – Interview questions** *(Thijs Timmerman, KPMG)*

**Appendix 5** – *SecurityScore Assessment* questionnaire

**Appendix 6** – *SecurityScore Assessment – Raw data*

**Appendix 7** – *Evaluation Reports in the following order:*

- *Energy Corp.*
- *Education_1 Corp.*
- *Education_2 Corp.*
- *Maritime Corp.*

## **Appendix 1 – Interview questions** *(Lillian Bøe, Marin IT AS)*

1. Was there any due diligence done to inspect and evaluate the existing IT Infrastructure of AGR (back in the day)?
There were several due diligence processes in that period of the sale for AGR Field Operations. We delivered all info we had about the infrastructure to the negotiators.
We werer working around the clock for several months

2. Was there any existing framework / pre-defined checklist used (by Oceaneering or evaluating party) to evaluate the IT Infrastructure of AGR?
I actually don't know who was asking for the information we produced. I think there were 3 different due diligences in the period.
I was working with check lists and I assume Oceaneering got the information.

3. Were there any specific IT Security policies, practices and technologies in use in AGR (back in the day)?
Yes there were. Security policies, Infrastructure framework, IT support, Client handling (SCCM)
We were working with the ITIL framework.

4. Was there any existing framework / pre-defined checklist used (by Oceaneering or evaluating party) to evaluate the IT Security posture of AGR?
Yes some.

5. Was AGR using more up to date technologies (as compared to Oceaneering) back in the day?
Ye. We always said it was like going 6 years back in time when we merged…. Oceaneering was still using Novell!

6. If yes, was it ever considered by Oceaneering to adopt the good policies and technologies in use by AGR to strengthen their IT Security posture?
No. Not really.

7. If yes, why? If no, why?
We tried to get them to use AD and to help them understand what knowledge and competence we had. But they never let us participate.

8. Do you feel that when two companies merge, the company with better IT Infrastructure and IT Security posture should get the precedence and the other merging party should adopt their model of IT technologies and practices?
Yes of course. But I guess it comes down to culture. Ocaneering never trusted a small entity as AGR to "tell them" how to operate.

## **Appendix 2 – Interview questions** *(Magnus Felde, Deloitte)*

*i) Approximately how many man hours are used to perform this analysis?*
*2) Do you have any fixed methodology to perfom this analysis or the modus operandi changes based on the factors like nature of the industry, scale, demographics, regional practices (cultural) etc.*

The topic of due diligence and cyber security is both interesting and relevant.

In terms of approach and man-hours, I'm afraid the answer is "it depends". But in general, it is key to understand what "elements" of the IT portfolio are to be merged / kept in the new company. Based on this, and the desired "target operating model" it might become more clear which policy make sense. In many M&A the case is that one of the two companies more or less remains the same, and relevant parts of the other company is merged into this. That said, research show that most M&A "fail" (the goal is not achieved). Merging two business cultures are often the key reason. However, one interesting question then is to what extent "mis-match" with regards to the new IT environment plays a role in this.

With regards to due diligence another consideration companies more and more seek to get good answers to is wether the Intellectual Property (IP) in fact is still secret, or if this had been stolen. The value of the company would/could then be heavily reduced. In such cases Deloitte can do so called Threat Hunting (with tool support) to try to identify if an attacker is already on the inside.

## **Appendix 3 – Interview questions** *(Kimberly Ng, Halfwave AS)*

1. In the bidding process, do the clients ask for Information Security related aspects from the vendors?

Yes, normally in the HSEQ part, we will be asked to comply to certain IT requirements and security

2. How much does it actually weigh while deciding a vendor (cost vs. information security preparedness)?

We believe that most reputable vendors should decent security so it's not top priority but if vendor is a small company that is not well known then audit will be done to ensure that they are up to the standards

3. Even after choosing a vendor, are the clients demanding about the adapting to their Information Security culture?

There are standards and regulations set, so they have to conform to it and comply to the NDA

4. Have you experienced any cyber incident that occurred via a vendor company (due to negligence or lack of knowledge of the vendor employee)?

None that i am aware of so far

5. Is there an Information Security credit score system in use at the moment to reflect on the Information Security preparedness of an organization (used in the bidding process)?

Nope.

6. Do you have any comments on the importance / influence of Information security posture of an organization (vendor) in bagging a contract?

I suppose it depends on what is the nature of the product or services that we are providing. In our case it might not be a top prioriothy

## **Appendix 4 – Interview questions** *(Thijs Timmerman, KPMG)*

*i) Approximately how many man hours are used to perform such analysis?*

That fully depends on factors like organisation size, aimed degree of integration, regulatory environment and level of detail of the due diligence. A general answer would be anywhere between 5 and 50 man days for such a due diligence effort – but for very big and complex mergers that can be even bigger (think of multiple business units as a multiplyer).

*2) Do you have any fixed methodology to perfom such analysis or the modus operandi changes based on the factors like nature of the industry, scale, demographics, regional practices (cultural) etc.*

Yes we do have multiple. A prominent factor you will need to include is the regulatory environment. If, for example, one of the two companies is not yet subject to certain industry regulations (e.g. financial oversight, healthcare standards, oil and gas supervisory), but will become that after a merger, then it is of crucial importance to perform due diligence on the regulatory gap.
The Cyber Maturity Assessment framework that we presented last year is one of the frameworks we use. More market-specific frameworks are KPMG IP so cannot be shared.

## **Appendix 5** – *SecurityScore Assessment* questionnaire

# Project: Information Security Posture Evaluation

This is a project being conducted by Ivan Talwar who is writing his Master Thesis with Norwegian University of Science and Technology (NTNU, Gjøvik).

Program name - Masters in Information Security (MIS)
Subject Code - IMT4900
Semester - Fall, 2019
Name of the Supervisor - Laura Georg Schaffner

Privacy Disclaimer:

- All the information that is collected during this activity will be anonymized and you/your organization will not be directly quoted if you direct us to do so.
- The data is stored securely and will not be shared with another party without your explicit consent.
- Once the purpose of this study is finished, all this data will be permanently deleted and you will receive a receipt stating the same.
- Once you have finished filling up the form, you will receive an Information Security rating and reasons for the same.
- Additionally, a list of recommendations / mitigation measures to ensure safety of your information assets.
- At any point in time, you can withdraw your consent and have us delete your information.
- Should you need an overview of your information as a data subject, you can always ask for a copy of it.

* Required

1. **I have read the privacy disclaimer and I understand my rights.** *
   *Mark only one oval.*

   ○ I accept *Skip to question 2.*

   ○ I do not accept. Please exit the form. *Stop filling out this form.*

## About you

Please provide the information so that the conclusions can be inferred.

2. **Your full name**

   ______________________

3. **Work Title** *

   ______________________

4. **Organization** *

   ______________________

5. **Your email address (will receive evaluation report here)** *

____________________________________

6. **Associated with sector** *

*Mark only one oval.*

○ Education
○ Energy
○ Healthcare
○ Others

7. **I wish to be anonymized in the research paper.** *

*Mark only one oval.*

○ Yes
○ No

## General Evaluation of Information Security Posture

Under general evaluation, we will be testing all aspects of an IT Infrastructure namely General Policies, Network, Storage, Servers, Application Development, Information Classification and Management.

You can easily answer the questions if you are hosting your infrastructure (on premise). This evaluation is based on the ISO/IEC 27001 standard and is considered to be the 'gold standard' in the industry.

Once you finish the evaluation, you will receive a PDF file with your evaluation results and some mitigation steps to improve the score. This evaluation can act like a bench marking exercise with some tips on improving your security posture.

NOTE: If your infrastructure (or a part of your infrastructure) is hosted by a Cloud Provider, please refer to your service contract (SLA) or contact them directly to see which risks are covered by them by default. Every cloud provider provides a common level of security to all its tenants which should mitigate some risks. The rest of the risks should ideally be evaluated locally and mitigated within the local infrastructure or at the client level.

## General Policies

A list of administrative / operational controls.

8. **1. Do you have a clear overview of all the IT assets (Asset Management) that exist in the organization (including but not limited to the SCADA devices)?** *

*Mark only one oval.*

○ Yes
○ No

9.

**2. Do you have any pre-defined Information security policy to ensure the confidentiality, integrity and availability of the information systems?** *

*Mark only one oval.*

○ Yes

○ No

10.

**3. Do you have dedicated Information Security roles as in a CISO or a Data Privacy Officer in your organization?** *

*Mark only one oval.*

○ Yes

○ No

11.

**4. Do you have a dedicated team working to detect and respond to security incidents – Security Operations Center (SOC) or an Incident Response Team (IRT)?** *

*Mark only one oval.*

○ Yes

○ No

12.

**5. Do you have a dedicated annual Information Security budget in your organization?** *

*Mark only one oval.*

○ Yes

○ No

13.

**6. Does your top management know about the organization's risk appetite and is actively engaged in making a roadmap for the future?** *

*Mark only one oval.*

○ Yes

○ No

14.

**7. Do you have a provision of an emergency fund in case of an event – to mitigate the issue on emergency basis?** *

*Mark only one oval.*

○ Yes

○ No

15.

**8. Do you perform due diligence on the information security posture of your future business partners or vendors?** *

*Mark only one oval.*

○ Yes

○ No

16.

**9. Do you have strict policy against bringing your own device and connected it to the organization network?** *

*Mark only one oval.*

○ Yes

○ No

17.

**10. Does your organization use multi-factor authentication?** *

*Mark only one oval.*

○ Yes

○ No

18.

**11. Do you have policy for issuing time bound credentials to the guest Wi-Fi network?** *

*Mark only one oval.*

○ Yes

○ No

19.

**12. Do all the workstations have a malware protection / endpoint security program installed?** *

*Mark only one oval.*

○ Yes

○ No

20.

**13. Do the users have local administrator rights on the workstations?** *

*Mark only one oval.*

○ Yes

○ No

21.

**14. Do you conduct regular user training and awareness campaigns to minimize security breaches that involve a human error? (Initiatives like Security month counts).** *

*Mark only one oval.*

○ Yes

○ No

22.

**15. Do you periodically conduct mock attacks like pseudo-phishing emails to your own IT users to check their knowledge and preparedness against such attempts?** *

*Mark only one oval.*

○ Yes

○ No

23.

**16. Do you perform vetting on the new employees – background check, security check etc.?** *

*Mark only one oval.*

○ Yes

○ No

24.

**17. Do you have any dedicated channels to report any possible insider threat?** *

*Mark only one oval.*

○ Yes

○ No

25.

**18. Do you make the new employees sign an NDA (Non-disclosure agreement) to ensure that all the trade secrets are kept safe?** *

*Mark only one oval.*

○ Yes

○ No

26.

**19. Do you have annual IT Audits for bench marking purposes or to retain security certifications?** *

*Mark only one oval.*

○ Yes

○ No

27.

**20. Do you have policies that can withstand in the court of law?** *

*Mark only one oval.*

○ Yes

○ No

28.

**21. Do you have full compliance to the local laws of the land like GDPR, Data Privacy Law etc.?** *

*Mark only one oval.*

○ Yes

○ No

29.

**22. Do you have a Business contingency plan in place, should there be an event?** *

*Mark only one oval.*

○ Yes

○ No

30.

**23. Do you have a Disaster Recovery Plan or a mechanism in place, should there be an incident?** *

*Mark only one oval.*

○ Yes

○ No

31.

**24. Do you perform Disaster recovery drills on an annual basis where all the stakeholders (teams) participate and check their preparedness / readiness to resume activity, should there be an incident?** *

*Mark only one oval.*

○ Yes

○ No

## Network

Network controls and architecture.

32.

**25. Do you have Virtual LANs (VLANs) setup on the switches for different devices? (For example – separate VLANs for workstations, printers, Wi-Fi, servers, video solutions etc.)** *

*Mark only one oval.*

○ Yes

○ No

33.

**26. Do you have MAC tagging enabled on the switch ports giving internet access to employees performing key functions like payroll, HR, finance etc.?** *

*Mark only one oval.*

○ Yes

○ No

34.

**27. Do you have 802.1x protocol enables at port level to force user authentication whenever the data passes through the port?** *

*Mark only one oval.*

○ Yes

○ No

35.

**28. Do you have an Access Control List (ACL) or any other form of routing table configured on your router to 'dynamically' assess and filter the data traffic (stateful routing)?** *

*Mark only one oval.*

○ Yes

○ No

36.

**29. Do you use internal DNS servers to route your network traffic (network translation)?**

*Mark only one oval.*

○ Yes

○ No

37.

**30. Do you have a network firewall that filters the data traffic by allowing and disallowing data traffic based on the pre-defined set of rules?** *

*Mark only one oval.*

○ Yes

○ No

38.

**31. Do you have a web security gateway that can inspect even the content of the data packets to make a decision on whether to allow or disallow a data packet dynamically?** *

*Mark only one oval.*

○ Yes

○ No

39.

**32. Do you have a stateful inspection firewall that keeps a record of any communication between an internal and an external host and can allow or disallow communication requests based on that historical data?** *

*Mark only one oval.*

○ Yes

○ No

40.

**33. Do you have a load balancing provisions enabled in your infrastructure on the assets being frequently used by the users to ensure availability?** *

*Mark only one oval.*

○ Yes

○ No

41.

**34. Do you have VPN concentrators to form encrypted VPN tunnels from outside of network?** *

*Mark only one oval.*

○ Yes

○ No

42.

**35. Do you have VPN setup on the router / firewall level to allow secure external connection to the internal network? (IPSec etc.)**

*Mark only one oval.*

○ Yes

○ No

43.

**36. Do you have Intrusion detection system in place to detect any malicious activity on the internal network?** *

*Mark only one oval.*

○ Yes

○ No

44.

**37. Do you have an automated response system should a malicious activity is detected (Intrusion Prevention System)?**

*Mark only one oval.*

○ Yes

○ No

45.

**38. Do you use any Protocol Analyzers (like Wireshark, Splunk etc.) to monitor the network traffic between points of interests (ex - a user connection to a confidential internal database etc.)?** *

*Mark only one oval.*

○ Yes

○ No

46.

**39. Does your network equipment filter traffic based on the validity of security certificates of a website i.e. revoked certificate websites are not accessible?** *

*Mark only one oval.*

○ Yes

○ No

47.

**40. Do you have an encrypted connection (tunnel) to any external network (which can be a sister company or a business partner) or another site configured at the gateway level?** *

*Mark only one oval.*

○ Yes

○ No

48.

**41. Do you use an MPLS connection for data traffic that needs to be transmitted on real time basis?**

*Mark only one oval.*

○ Yes

○ No

○ Not Applicable since integrity of the data on real time is not important to us

49.

**42. Do you have special security measures in place for internet facing services (example a demilitarized zone or a DMZ)?**

*Mark only one oval.*

○ Yes

○ No

## Storage

Network-attached storage (NAS) - storage, encryption, back up and access controls.

50.

**43. Do you have a backed-up copy of all the data stored on the network resources at all times?** *

*Mark only one oval.*

○ Yes

○ No

51\.

**44. Do you have redundancy of the storage units – in datacenters or on cloud to ensure fail-over in case of an event?** *

*Mark only one oval.*

○ Yes

○ No

52\.

**45. Do you have physical security (guards etc.) in place at the places where the storage equipment is kept?** *

*Mark only one oval.*

○ Yes

○ No

53\.

**46. Do you have other forms of security controls (like access cards, biometric scans etc.) to ensure safety of the storage equipment?** *

*Mark only one oval.*

○ Yes

○ No

54\.

**47. Have you enabled disk encryption across your organization (via tools like Bitlocker)?** *

*Mark only one oval.*

○ Yes

○ No

55\.

**48. Is the data (media) stored on the cellphones encrypted via Mobile Device Management (MDM) solutions or standalone devices?** *

*Mark only one oval.*

○ Yes

○ No

56\.

**49. Do you have video surveillance available for the places where storage/network equipment is stored?** *

*Mark only one oval.*

○ Yes

○ No

57.

**50. Do you have provisions to log user activity and store it while they access these storage devices? (to set accountability)** *

*Mark only one oval.*

○ Yes

○ No

## Servers

Security on servers, accessibility, authentication, elevated access (privileged elevated access accounts) etc.

58.

**51. Do all the servers have the internet access?** *

*Mark only one oval.*

○ Yes

○ No

59.

**52. Do the servers have any controls that blocks installation of new programs on the servers (for example – Carbon Black which needs an explicit approval on the MD5 checksum value of every file being executed)?** *

*Mark only one oval.*

○ Yes

○ No

60.

**53. Do you have redundant servers to ensure availability and disaster recovery?** *

*Mark only one oval.*

○ Yes

○ No

61.

**54. Do you have OS patch management system in place – installing security patches during a maintenance window to ensure the safety of the systems?** *

*Mark only one oval.*

○ Yes

○ No

62.

**55. Do you have separate types of user accounts – one to access workstation and other provisional accounts to access infrastructure management resources like servers?** *

*Mark only one oval.*

○ Yes

○ No

63.

**56. Do you have two (or three) factor authentication to harden the authentication process?** *

*Mark only one oval.*

○ Yes

○ No

64.

**57. Is multiple factor authentication enabled to remotely access the servers?** *

*Mark only one oval.*

○ Yes

○ No

65.

**58. Do you have malware protection installed on the servers?** *

*Mark only one oval.*

○ Yes

○ No

66.

**59. Do you have any other form of intrusion detection system available on the servers that would raise a security flag, should there be any malicious activity detected?** *

*Mark only one oval.*

○ Yes

○ No

67.

**60. Do you have processes to periodically check if the user accounts have been properly terminated once an employee leaves? It is very important in case of provisional (prv) accounts with elevated access.** *

*Mark only one oval.*

○ Yes

○ No

## Applications

Secure Development practices, Security by design etc.

68.

**61. Do you have an application development team to maintain and update the in-house applications?** *

*Mark only one oval.*

○ Yes

○ No

○ Not Applicable

69.

**62. Do you program in-house application using “secure by design” approach?** *

*Mark only one oval.*

○ Yes

○ No

○ Not Applicable

70.

**63. Are the applications in use by your organization periodically updated/patched based on the changing threat landscape?** *

*Mark only one oval.*

○ Yes

○ No

71.

**64. Are these applications tested for any vulnerabilities from the security point of view (techniques like penetration testing, risk assessment, Data Privacy Impact Assessment- DPIA etc.)?** *

*Mark only one oval.*

○ Yes

○ No

## Information classification and management

Access controls, data classification, storage and sharing, reporting breaches etc.

72.

**65. Do you have a good overview of the information assets that you possess?** *

*Mark only one oval.*

○ Yes

○ No

73.

**66. Do you have good access control mechanisms in place so that only authorized employees can access the information?** *

*Mark only one oval.*

○ Yes

○ No

74.

**67. Have you differentiated the information based on the criticality like terming documents are classified, confidential, private, de-classified etc. (following some model like Bell-La Padula, Chinese wall etc.)?** *

*Mark only one oval.*

○ Yes

○ No

75.

**68. Do you have a clear desk policy – where the confidential information is not kept openly on the desk for other to be seen or left by the printers / fax machines?** *

*Mark only one oval.*

○ Yes

○ No

76.

**69. Do you have other confidentiality measures like secure printing – print job will be finished only when the person physically shows up at the printer?** *

*Mark only one oval.*

○ Yes

○ No

77.

**70. Do you use any other form of document control system like SharePoint, box, Google drive etc. for version control, collaboration or integrity check?** *

*Mark only one oval.*

○ Yes

○ No

**Appendix 6** – *SecurityScore Assessment – Raw data*

| | | | | |
|---|---|---|---|---|
| Timestamp | 11.29.2019 10:19:36 | 12.2.2019 13:02:07 | 12.2.2019 14:31:25 | 12.3.2019 22:29:53 |
| I have read the privacy disclaimer and I understand my rights. | I accept | I accept | I accept | I accept |
| Your full name | Person 1 | Person 2 | Person 3 | Person 4 |
| Work Title | Leader IT Operations | Senior Network Consultant | IT Manager | Senior IT Consultant |
| Organization | Education 1 | Maertime 1 | Education 2 | Energy 1 |
| Your email address (will receive evaluation report here) | <hidden> | <hidden> | <hidden> | <hidden> |
| Associated with sector | Education | Maritime | Education | Energy |
| I wish to be anonymized in the research paper. | Yes | Yes | Yes | Yes |
| 1.Do you have a clear overview of all the IT assets (Asset Management) that exist in the organization (including but not limited to the SCADA devices)? | No | Yes | No | No |
| 2.Do you have any pre-defined Information security policy to ensure the confidentiality, integrity and availability of the information systems? | No | Yes | Yes | Yes |
| 3.Do you have dedicated Information Security roles as in a CISO or a Data Privacy Officer in your organization? | Yes | Yes | No | No |
| 4.Do you have a dedicated team working to detect and respond to security incidents – Security Operations Center (SOC) or an Incident Response Team (IRT)? | No | Yes | Yes | No |
| 5.Do you have a dedicated annual Information Security budget in your organization? | Yes | Yes | No | No |
| 6.Does your top management know about the organization’s risk appetite and is actively engaged in making a roadmap for the future? | No | Yes | Yes | No |
| 7.Do you have a provision of an emergency fund in case of an event – to mitigate the issue on emergency basis? | Yes | Yes | No | No |
| 8.Do you perform due diligence on the information security posture of your future business partners or vendors? | No | Yes | Yes | No |
| 9.Do you have strict policy against bringing your own device and connected it to the organization network? | No | Yes | No | No |
| 10.Does your organization use multi-factor authentication? | Yes | Yes | Yes | Yes |
| 11.Do you have policy for issuing time bound credentials to the guest Wi-Fi network? | No | No | Yes | No |
| 12.Do all the workstations have a malware protection / endpoint security program installed? | Yes | Yes | Yes | Yes |
| 13.Do the users have local administrator rights on the workstations? | No | No | No | Yes |
| 14.Do you conduct regular user training and awareness campaigns to minimize security breaches that involve a human error? (Initiatives like Security month counts). | Yes | Yes | Yes | No |
| 15.Do you periodically conduct mock attacks like pseudo-phishing emails to your own IT users to check their knowledge and preparedness against such attempts? | No | Yes | No | No |
| 16.Do you perform vetting on the new employees – background check, security check etc.? | No | Yes | No | No |
| 17.Do you have any dedicated channels to report any possible insider threat? | No | Yes | Yes | No |
| 18.Do you make the new employees sign an NDA (Non-disclosure agreement) to ensure that all the trade secrets are kept safe? | No | Yes | Yes | Yes |
| 19.Do you have annual IT Audits for bench marking purposes or to retain security certifications? | No | Yes | No | No |
| 20.Do you have policies that can withstand in the court of law? | Yes | Yes | Yes | No |
| 21.Do you have full compliance to the local laws of the land like GDPR, Data Privacy Law etc.? | No | Yes | Yes | No |
| 22.Do you have a Business contingency plan in place, should there be an event? | Yes | Yes | Yes | No |
| 23.Do you have a Disaster Recovery Plan or a mechanism in place, should there be an incident? | No | Yes | Yes | No |
| 24.Do you perform Disaster recovery drills on an annual basis where all the stakeholders (teams) participate and check their preparedness / readiness to resume activity, should there be an incident? | No | Yes | No | No |
| 25.Do you have Virtual LANs (VLANs) setup on the switches for different devices? (For example – separate VLANs for workstations, printers, Wi-Fi, servers, video solutions etc.) | Yes | Yes | Yes | Yes |
| 26.Do you have MAC tagging enabled on the switch ports giving internet access to employees performing key functions like payroll, HR, finance etc.? | No | Yes | No | No |
| 27.Do you have 802.1x protocol enables at port level to force user authentication whenever the data passes through the port? | No | No | Yes | No |
| 28.Do you have an Access Control List (ACL) or any other form of routing table configured on your router to 'dynamically' assess and filter the data traffic (stateful routing)? | Yes | No | Yes | No |
| 29.Do you use internal DNS servers to route your network traffic (network translation)? | Yes | Yes | Yes | Yes |
| 30.Do you have a network firewall that filters the data traffic by allowing and disallowing data traffic based on the pre-defined set of rules? | Yes | Yes | Yes | Yes |

| | | | | |
|---|---|---|---|---|
| **31.Do you have a web security gateway that can inspect even the content of the data packets to make a decision on whether to allow or disallow a data packet dynamically?** | No | Yes | Yes | Yes |
| **32.Do you have a stateful inspection firewall that keeps a record of any communication between an internal and an external host and can allow or disallow communication requests based on that historical data?** | Yes | Yes | Yes | No |
| **33.Do you have a load balancing provisions enabled in your infrastructure on the assets being frequently used by the users to ensure availability?** | Yes | Yes | Yes | No |
| **34.Do you have VPN concentrators to form encrypted VPN tunnels from outside of network?** | Yes | Yes | Yes | Yes |
| **35.Do you have VPN setup on the router / firewall level to allow secure external connection to the internal network? (IPSec etc.)** | Yes | Yes | Yes | Yes |
| **36.Do you have Intrusion detection system in place to detect any malicious activity on the internal network?** | Yes | Yes | Yes | No |
| **37.Do you have an automated response system should a malicious activity is detected (Intrusion Prevention System)?** | No | Yes | Yes | No |
| **38.Do you use any Protocol Analyzers (like Wireshark, Splunk etc.) to monitor the network traffic between points of interests (ex - a user connection to a confidential internal database etc.)?** | No | Yes | Yes | No |
| **39.Does your network equipment filter traffic based on the validity of security certificates of a website i.e. revoked certificate websites are not accessible?** | No | Yes | Yes | No |
| **40.Do you have an encrypted connection (tunnel) to any external network (which can be a sister company or a business partner) or another site configured at the gateway level?** | Yes | Yes | Yes | Yes |
| **41.Do you use an MPLS connection for data traffic that needs to be transmitted on real time basis?** | Not Applicable since integrity of the data on real time is not important to us | No | Yes | No |
| **42.Do you have special security measures in place for internet facing services (example a demilitarized zone or a DMZ)?** | Yes | Yes | Yes | Yes |
| **43.Do you have a backed-up copy of all the data stored on the network resources at all times?** | Yes | Yes | Yes | Yes |
| **44.Do you have redundancy of the storage units – in datacenters or on cloud to ensure fail-over in case of an event?** | Yes | Yes | Yes | Yes |
| **45.Do you have physical security (guards etc.) in place at the places where the storage equipment is kept?** | Yes | Yes | No | Yes |
| **46.Do you have other forms of security controls (like access cards, biometric scans etc.) to ensure safety of the storage equipment?** | Yes | Yes | Yes | Yes |
| **47.Have you enabled disk encryption across your organization (via tools like Bitlocker)?** | No | Yes | Yes | Yes |
| **48.Is the data (media) stored on the cellphones encrypted via Mobile Device Management (MDM) solutions or standalone devices?** | No | No | Yes | No |
| **49.Do you have video surveillance available for the places where storage/network equipment is stored?** | Yes | Yes | No | Yes |
| **50.Do you have provisions to log user activity and store it while they access these storage devices? (to set accountability)** | No | Yes | Yes | No |
| **51.Do all the servers have the internet access?** | Yes | No | No | Yes |
| **52.Do the servers have any controls that blocks installation of new programs on the servers (for example – Carbon Black which needs an explicit approval on the MD5 checksum value of every file being executed)?** | No | Yes | No | Yes |
| **53.Do you have redundant servers to ensure availability and disaster recovery?** | Yes | Yes | Yes | Yes |
| **54.Do you have OS patch management system in place – installing security patches during a maintenance window to ensure the safety of the systems?** | Yes | Yes | Yes | Yes |
| **55.Do you have separate types of user accounts – one to access workstation and other provisional accounts to access infrastructure management resources like servers?** | Yes | Yes | Yes | Yes |
| **56.Do you have two (or three) factor authentication to harden the authentication process?** | Yes | Yes | Yes | No |
| **57.Is multiple factor authentication enabled to remotely access the servers?** | No | Yes | Yes | Yes |
| **58.Do you have malware protection installed on the servers?** | Yes | Yes | Yes | Yes |
| **59.Do you have any other form of intrusion detection system available on the servers that would raise a security flag, should there be any malicious activity detected?** | No | Yes | Yes | No |
| **60.Do you have processes to periodically check if the user accounts have been properly terminated once an employee leaves? It is very important in case of provisional (prv) accounts with elevated access.** | No | Yes | Yes | No |
| **61.Do you have an application development team to maintain and update the in-house applications?** | Yes | Yes | Not Applicable | Not Applicable |

| | | | | |
|---|---|---|---|---|
| **62.Do you program in-house application using “secure by design” approach?** | Yes | Yes | Not Applicable | Not Applicable |
| **63.Are the applications in use by your organization periodically updated/patched based on the changing threat landscape?** | No | Yes | Yes | Yes |
| **64.Are these applications tested for any vulnerabilities from the security point of view (techniques like penetration testing, risk assessment, Data Privacy Impact Assessment- DPIA etc.)?** | No | Yes | Yes | No |
| **65.Do you have a good overview of the information assets that you possess?** | No | Yes | Yes | No |
| **66.Do you have good access control mechanisms in place so that only authorized employees can access the information?** | Yes | Yes | Yes | Yes |
| **67.Have you differentiated the information based on the criticality like terming documents are classified, confidential, private, de-classified etc. (following some model like Bell-La Padula, Chinese wall etc.)?** | No | Yes | No | No |
| 68.Do you have a clear desk policy – where the confidential information is not kept openly on the desk for other to be seen or left by the printers / fax machines? | No | Yes | Yes | No |
| 69.Do you have other confidentiality measures like secure printing – print job will be finished only when the person physically shows up at the printer? | Yes | Yes | No | No |
| 70.Do you use any other form of document control system like SharePoint, box, Google drive etc. for version control, collaboration or integrity check? | Yes | Yes | Yes | Yes |

**Appendix 7** – *Evaluation Reports  in the following order (See attached files):*

- *Energy Corp.*
- *Education_1 Corp.*
- *Education_2 Corp.*
- *Maritime   Corp.*

**Names have been changed due to privacy concerns of the subjects.*

**Energy Corp.**

*Q4, 2019*

SECURITY | SCORE

BY IVAN@NTNU

Issued by **Ivan Talwar**

*MIS, NTNU (Gjøvik)*

SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Summary Report

## Provided to

*Energy Corp.*

## Issuer (on behalf of NTNU)

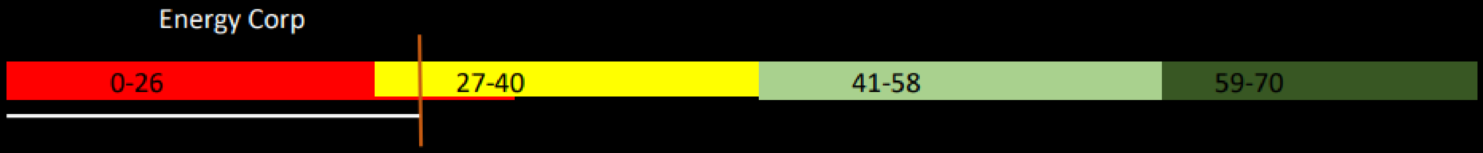
Ivan Talwar

## Date

December 05, 2019

## Your estimated score is

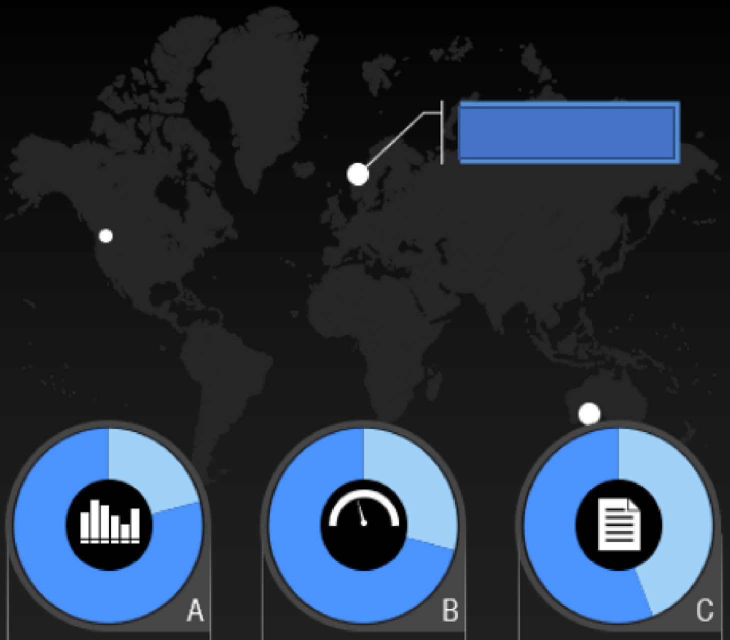
**29*** out of **71**



## Areas of Improvement

52%

Your security posture needs remarkable improvement especially in the Policies, Information Management and Network Architecture areas. We will provide some basic mitigation steps that, if followed, should help improve your security posture.



79%

Polices

- Asset Management
- Stricter BYOD policy
- Awareness amongst employees

71%

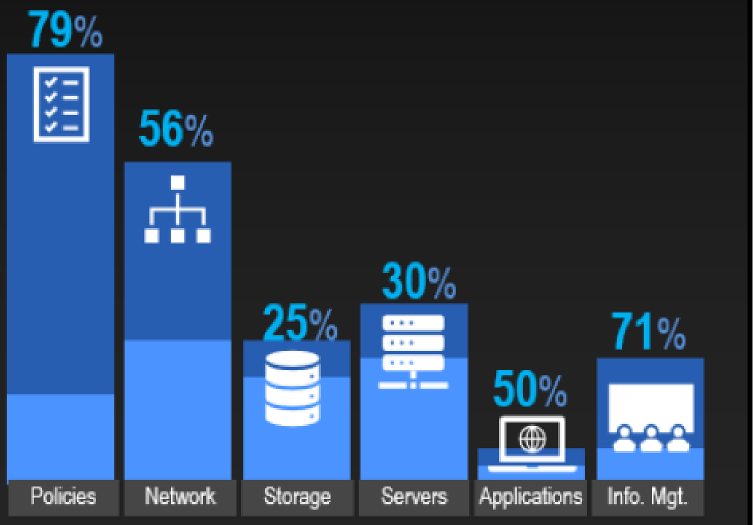
Info. Mgt

- Poor overview of info assets
- Incident Reporting system

56%

Network

- Lack of a stateful firewall
- MAC tagging for critical job functions like HR, Payroll etc.



SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Threat Landscape Report
## (Sector based)

## 55% Threat agent based exposure

This is [redacted] threat exposure score. This is based on the sector-specific risks. Some of the relevant risks have been mentioned that are applicable to the entire education sector.

**Typical assets for Energy Sector**

- Research data on energy reserves (inspection activities, etc.)
- SCADA devices (Commercia control systems/CNC machines)
- Business deals – information on bids, contracts. etc.
- Market Analysis
- Personal information of decision making executives
- Information on new technologies (Intellectual Property)

### Nation-states

**Risk 1**: Nation-states might acquire exploration data on energy assets of a nation.

**Risk 2**: Nation-states might acquire confidential information on deals between public and private sector entities.

**Risk 3**: Nation-states might seek personally identifiable information (PII) on key personnel in an energy deal.

**Risk 4**: Nation-states might disrupt the daily extraction/processing operations to synthetically manipulate the energy prices or set a monopoly in the sector.

**Risk 5**: Nation-states might cause disruption by infecting the CNC machines (thus SCADA devices) like in case of Stuxnet.

### Cyber-Criminals

**Risk 1**: Cyber-criminals might acquire exploration data on energy assets of a nation and sell it to other nations who can benefit from it.

**Risk 2**: Cyber-criminals might acquire confidential information on deals between public and private sector entities and sell it further to other (enemy) states which can further be leveraged.

**Risk 3**: Cyber-criminals might seek personally identifiable information (PII) on key personnel in an energy deal sell it further to other (enemy) states which can further be leveraged.

**Risk 4**: Cyber-criminals might disrupt the daily extraction/processing operations to synthetically manipulate the energy prices or set a monopoly in the sector (paid by companies or nation-states).

**Risk 5**: Cyber-criminals might cause disruption by targeting the CNC machines (thus SCADA devices) like in case of Stuxnet. [52] on the instructions of other (enemy) nation-states or business rivals.

**Risk 6**: Cyber-criminals might cause disruption via. Denial of service attacks to deface the energy sector firms; as directed.

**Risk 7**: Cyber-criminals might look at vendor network as an attack vector or a backdoor to main target's network, as happened in the case of Stuxnet

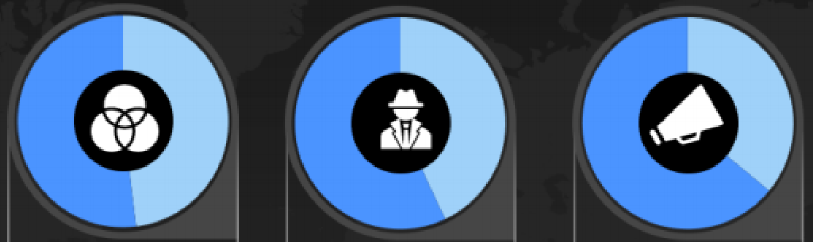
### Hacktivists

**Risk 1**: Hacktivists might cause disruption by bringing down the website with Denial of Service (DoS) / Distributed Denial of Service (DDoS) attacks or by planting a ransomware on the host company's network as an act of protest on some social issue.

**Risk 2**: Hacktivists might deface the energy company by taking control of the customer-facing interfaces and post messages in accordance to their agenda.

## Areas of Improvement

*(Based on the threat landscape for Energy sector)*



**52%**
Nation-states
Skill: high
Resource: full
Will: high
Motive: nationalistic

**57%**
Cyber-criminals
Skill: medium-high
Resource: medium-full
Will: medium-high
Motive: monetary

**64%**
Hacktivists
Skill: low-medium
Resource: low-medium
Will: medium-high
Motive: social

### Positives

- A pre-defined information Security policy
- Network segmentation for optimization of data traffic security
- Dynamic Intrusion Prevention controls
- Redundancy on storage to ensure availability
- Physical security controls on datacenter
- Encrypted drives to mitigate theft incidents
- File level (hashing) security for explicit approval for execution of a file
- Segregation of regular user accounts and administrator accounts
- Patch Management

### Areas of improvement

- Lack of overview on all IT Assets (Asset management)
- Lack of SOC or IRT functions for continuous monitoring and response.
- Leadership unaware of the risk appetite of the organization
- No due diligence on business partners
- Lack of vetting processes prior to employment of key personnel
- Lack of regulatory compliance (Data Privacy laws) on the applications used
- Lack of resilience testing of the Disaster recovery controls
- No defined mechanism for data classification
- Lack of measures like secure printing to ensure confidentiality of information.

# Recommendations

## (Based on ISO /IEC 27001 standard)

### Policies

- Use of *Asset Management* system can assist in better overview of threats and risks.
- Consider developing inhouse SOC/IRT capabilities or signing up for SECaaS *(Security as a Service).*
- Engaging leadership in the risk management activities can create awareness amongst the top executives about organizations' risk appetite and assist in better securing information security budget.
- Consider doing due-diligence on future business partners as they will get access your inhouse systems and if they are not sufficiently secure, they will increase your attack surface.
- Consider implementing a strict BYOD policy to ensure that infected devices are not introduced to your network.
- While generating guest accounts, consider making them timebound so that they cannot be re-used and misused.
- Consider engaging IT users in secure use of IT equipment practices by creating awareness – intranet articles about any ongoing Security cases, best practices against attempts of phishing or social engineering, etc.
- Consider establishing a vetting process at organizational level for personnel to be hired in key positions or functions.
- Consider conducting a DPIA on all your information collection, processing and storing systems to ensure regulatory compliance.
- Consider making a BCP / DR plan to ensure continuity of operations and ensure availability which is mission critical in education sector.

### Storage

- Consider enabling disk encryption on the computers to ensure mitigation in the event of computer theft.
- Consider data encryption on Mobile devices as well (tools like *Mobile Device Management* solutions can be useful).
- Consider saving the logs every time storage resources are accessed to ensure accountability.
- Consider adopting md5 security solutions on workstations where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.

### Applications

- Consider develop routines to check if all the accounts are terminated when not needed anymore – for employees, guests, vendors, consultants, etc.
- Consider developing a patch management routine or a workflow to install them periodically and also on emergency basis.

### Network

- Consider MAC tagging on the switch ports to avoid spoofing for business-critical functions like HR, CFO, CEO, etc.
- Consider enabling 802.1x (or similar protocols) on the switch port so that even if somebody gains unauthorized access to the building, he will still need to authenticate to access internet.
- Consider investing in real time monitoring, sandbox testing, responding and updating tool for dynamic intrusion prevention.
- Consider establishing redundancy in the networks and systems to ensure business continuity and can possibly be used for load balancing too.
- In the firewall, disallow/flag websites with expired security certificates as such sites are often used for malicious purposes.
- Consider adopting services like MPLS for functions that require real time data to ensure data integrity.

### Servers

- Consider adopting md5 security solutions on servers where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.
- Enable multiple factor authentication (atleast on the servers) to ensure that any attempts of authorized access can be mitigated.
- Endpoint protection or strict firewall rules with real time alerts, should there be an intrusion or even an attempt.

### Information Management

- Consider doing a *Data Privacy Impact Assessment* (DPIA) on all information systems to ensure regulatory compliance.
- Consider adopting a security incident reporting tool.
- Consider structuring your data on a department level (on three levels – public, shared and private) that will give you a better insight into your data assets and appropriate access controls can be instated subsequently.
- Consider adopting a clear-desk policy to ensure that unauthorized individuals don't get access to confidential information.

18476( 1)
18437( 1)
4th
3th
18594 ( 1)
18589 ( 4)
18590 ( 1)
18567 ( 2)
18567 ( 9)
18560 ( 5)
18514 ( 1)
18390 ( 1)
tically updated during trad
18440
18357
Bid (Qty)
Ask (Qty)
Chg
18590( 2)
18591( 1)
18588( 1)
-60
-70
-68
-92

**Education_1 Corp.**

*Q4, 2019*

SECURITY | SCORE

BY IVAN@NTNU

Issued by **Ivan Talwar**

*MIS, NTNU (Gjøvik)*

SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Summary Report

## Provided to

*Edication_1 Corp.*

## Issuer (on behalf of NTNU)

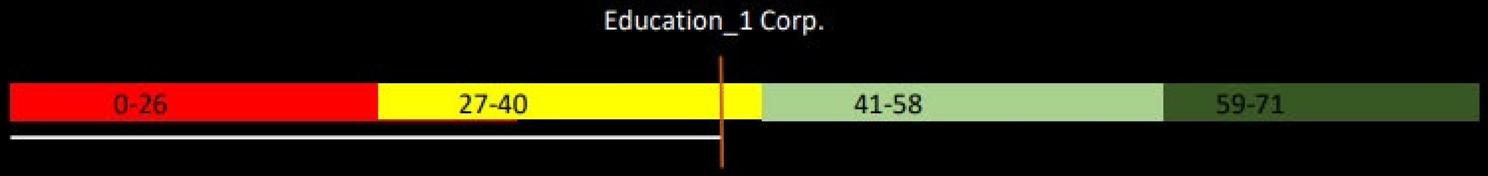
Ivan Talwar

## Date

December 05, 2019

## Your estimated score is

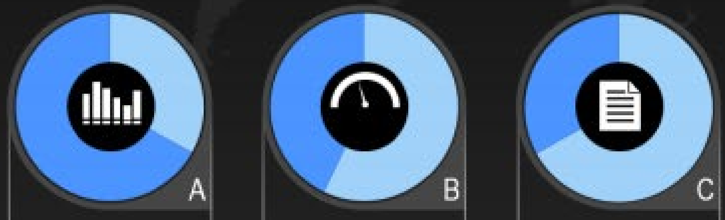
**38* out of 71**



## Areas of Improvement

45%

Your security posture needs remarkable improvement especially in the Policies, Information Management and Network Architecture areas. We will provide some basic mitigation steps that, if followed, should help improve your security posture.



67%

Polices

- Asset Management
- Risk Assessment
- Regulatory Compliance
- BCP / DR Preparedness

43%

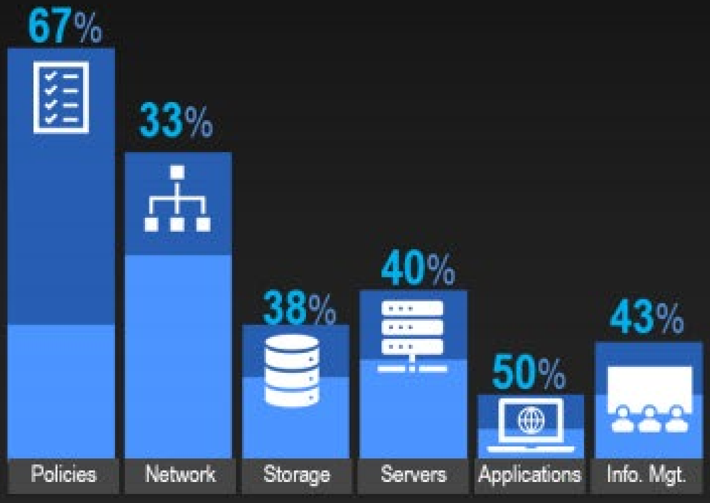
Info. Mgt

- Data identification and classification
- Better access Control mechanisms

33%

Network

- Lack of a stateful firewall
- MAC tagging for critical job functions like HR, Payroll etc.



SECURITY | SCORE
BY IVAN@NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Threat Landscape Report
## (Sector based)

## 48% Threat agent based exposure

This is [redacted] threat exposure score. This is based on the sector-specific risks. Some of the relevant risks have been mentioned that are applicable to the entire education sector.

**Typical assets for Education Sector**
- Sector-wide networks (like *Janet in UK and Uninett in Norway*)
- Intellectual Property (Research)
- Student Administration systems
- Computers and Servers / LMS
- Personal Information about Employees and Students
- Reputation

### Nation-states

**Risk 1**: Nation-states might try to obfuscate their digital footprint and avoid attribution.

**Risk 2**: Nation-states trick the genuine users in giving away their passwords in order to gain access to network.

**Risk 3**: Nation-states might try to steal intellectual property of the education institutions. This is mainly research work.

**Risk 4**: Nation-states might try to steal the PII about the students and staff to leverage it in forcing them into unethical practices, espionage etc.

**Risk 5**: Nation-states might try to utilize the computational power associated with the educational institutes to carry out DDoS attacks against enemy states.

### Cyber-Criminals

**Risk 1**: Cyber-criminals might try to obfuscate their digital footprint and avoid attribution.

**Risk 2**: Cyber-criminals trick the genuine users in giving away their passwords in order to gain access to network.

**Risk 3**: Cyber-criminals might try to steal intellectual property of the education institutions. This is mainly research work.

**Risk 4**: Cyber-criminals might try to steal the PII about the students and staff to sell it on illegal platforms like Dark-web.

**Risk 5**: Cyber-criminals might try to inject false information in the student administration or LMS systems (like false grades, credits etc.) for monetary gains.

**Risk 6**: Cyber-criminals might try to utilize the computational power associated with the educational institutes to carry out DDoS attacks against warranted entities and for crypto mining.

**Risk 7**: Cyber-criminals might get paid from the competitors to deface their opponents or tarnish their image for business gains by sabotaging the customer facing interfaces.

### Hacktivists

**Risk 1**: Hacktivists might sabotage the financial well-being indirectly by attacking a school and creating a bad reputation for them.

**Risk 2**: Hacktivist might attack a school to prove their point or as a sign of protest against that institution (against raging matters like expensive education, institutions stand on certain matters, etc.)

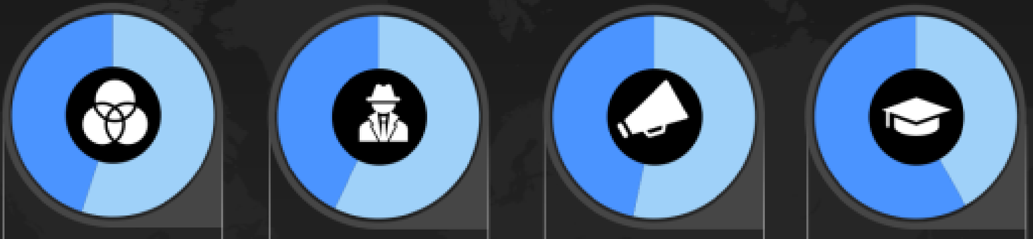
### Students

**Risk 1**: Students might Risk 1: Students might sabotage the reputation of the school reputation as an act of retaliation or to prove a point.

**Risk 2**: Students might try to gain unauthorized access to the student administration systems & change their grades, credits etc.). sabotage the reputation of the school reputation as an act of retaliation or to prove a point.
Risk 2: Students might try to gain unauthorized access to the student administration systems & change their grades, credits etc.).

## Areas of Improvement

(*Based on the threat landscape for Education sector*)



45%
Nation-states
Skill: high
Resource: full
Will: high
Motive: nationalistic

45%
Cyber-criminals
Skill: medium-high
Resource: medium-full
Will: medium-high
Motive: monetary

54%
Hacktivists
Skill: low-medium
Resource: low-medium
Will: medium-high
Motive: social

50%
Students
Skill: medium-high
Resource: low
Will: low
Motive: learning or amusement

### Positives

- Regular user training and awareness programs
- Detailed *Business Contingency Plan (BCP)* in place
- Segmented networks and managed routing practices
- Dynamic intrusion prevention
- Redundancy and load-balancing for high performance and availability
- MFA enabled on the IT Infrastructure
- Good access control mechanisms
- Document version control to ensure integrity.

### Areas of improvement

- Lack of overview on all IT Assets (Asset management)
- Lack of an information security policy
- Lack of an SOC or IRT function for continuous monitoring and support
- Lack of awareness in the executive management about the risk appetite.
- Lack of resilience testing of the Disaster recovery controls
- Lack of an overview over the Information Assets
- No defined mechanism for data classification

# Recommendations

## (Based on ISO /IEC 27001 standard)

### Policies

- Use of *Asset Management* system can assist in better overview of threats and risks.
- A well-defined Information Security policy can assist in secure practices and regulatory compliance.
- Consider developing or adopting SOC/IRT services. In Norway, Uninett provides such services to all educational institutions.
- Engaging leadership in the risk management activities can create awareness amongst the top executives about organizations' risk appetite and assist in better securing information security budget.
- Consider doing due-diligence on future business partners as they will get access your inhouse systems and if they are not sufficiently secure, they will increase your attack surface.
- Consider implementing a strict BYOD policy to ensure that infected devices are not introduced to your network.
- While generating guest accounts, consider making them timebound so that they cannot be re-used and misused.
- Consider conducting a DPIA on all your information collection, processing and storing systems to ensure regulatory compliance.
- Consider making a BCP / DR plan to ensure continuity of operations and ensure availability which is mission critical in education sector.

### Storage

- Consider enabling disk encryption on the computers to ensure mitigation in the event of computer theft.
- Consider data encryption on Mobile devices as well (tools like *Mobile Device Management* solutions can be useful).
- Consider saving the logs every time storage resources are accessed to ensure accountability.
- Consider adopting md5 security solutions on workstations where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.

### Applications

- Consider develop routines to check if all the accounts are terminated when not needed anymore – for employees, guests, vendors, consultants, etc.
- Consider developing a patch management routine or a workflow to install them periodically and also on emergency basis.

### Network

- Consider MAC tagging on the switch ports to avoid spoofing for business-critical functions like HR, CFO, CEO, etc.
- Consider enabling 802.1x (or similar protocols) on the switch port so that even if somebody gains unauthorized access to the building, he will still need to authenticate to access internet.
- Consider investing in real time monitoring, sandbox testing, responding and updating tool for dynamic intrusion prevention.
- In the firewall, disallow/flag websites with expired security certificates as such sites are often used for malicious purposes.

### Servers

- Consider adopting md5 security solutions on servers where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.
- Enable multiple factor authentication (atleast on the servers) to ensure that any attempts of authorized access can be mitigated.
- Endpoint protection or strict firewall rules with real time alerts, should there be an intrusion or even an attempt.

### Information Management

- Consider doing a *Data Privacy Impact Assessment* (DPIA) on all information systems to ensure regulatory compliance.
- Consider structuring your data on a department level (on three levels – public, shared and private) that will give you a better insight into your data assets and appropriate access controls can be instated subsequently.
- Consider adopting a clear-desk policy to ensure that unauthorized individuals don't get access to confidential information.

18476( 1)
-68
-0.36%
18437( 1)
-92
-0.50%
4th
3th
18594 ( 1)
18589 ( 4)
18590 ( 1)
18567 ( 2)
18567 ( 9)
18560 ( 5)
18514 ( 1)
18390 ( 1)
ically updated during trad
18440
18357
Bid (Qty)
Ask (Qty)
Chg
18590( 2)
18591( 1)
-60
-0.32%
-70
-0.37%
18588( 1)

**Education_2 Corp.**

*Q4, 2019*

SECURITY | SCORE

BY IVAN@NTNU

Issued by **Ivan Talwar**

*MIS, NTNU (Gjøvik)*

SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Summary Report

## Provided to

*Education_2 Corp.*

## Issuer (on behalf of NTNU)

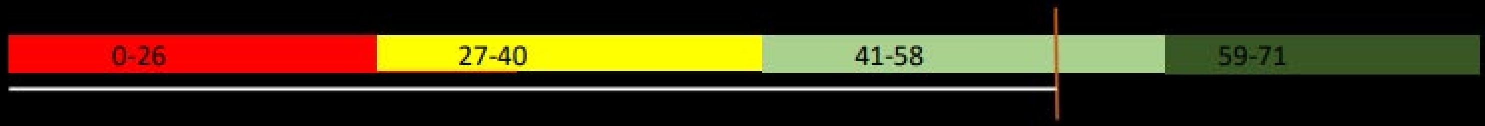
Ivan Talwar

## Date

December 05, 2019

## Your estimated score is

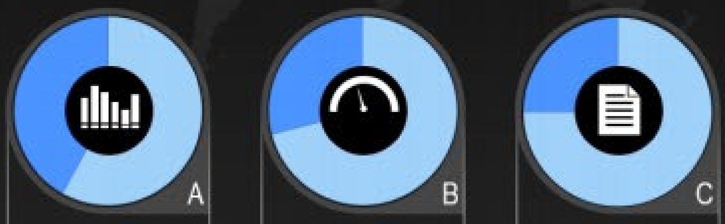
**53*** out of **71**



## Areas of Improvement

29%

Your security posture needs moderate levels of improvement especially in the Policies, Information Management and Network Architecture areas. We will provide some basic mitigation steps that, if followed, should help improve your security posture.



42%

Polices

- Asset Management
- Risk Assessment
- Regulatory Compliance
- BCP / DR Preparedness

29%

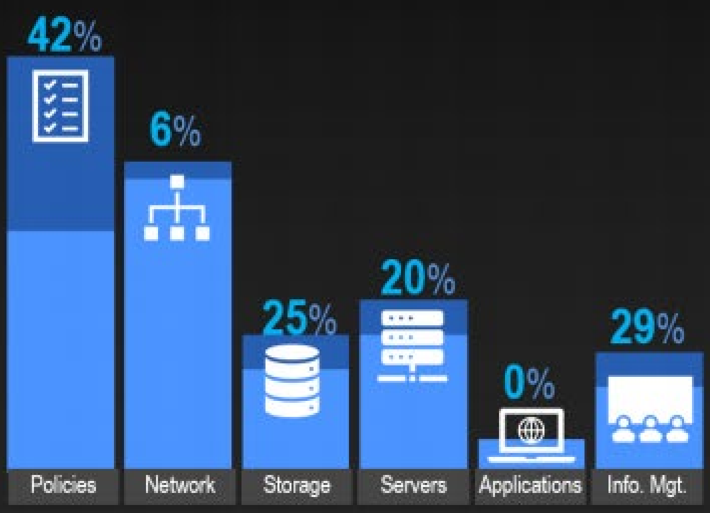
Info. Mgt

- Data identification and classification
- Better access Control mechanisms

25%

Storage

- Lack of a stateful firewall
- MAC tagging for critical job functions like HR, Payroll etc.



SECURITY | SCORE
BY IVAN@NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Threat Landscape Report (Sector based)

## 22% Threat agent based exposure

This is [redacted] threat exposure score. This is based on the sector-specific risks. Some of the relevant risks have been mentioned that are applicable to the entire education sector.

**Typical assets for Education Sector**

- Sector-wide networks (like *Janet in UK and Uninett in Norway*)
- Intellectual Property (Research)
- Student Administration systems
- Computers and Servers / LMS
- Personal Information about Employees and Students
- Reputation

### Nation-states

**Risk 1**: Nation-states might try to obfuscate their digital footprint and avoid attribution.

**Risk 2**: Nation-states trick the genuine users in giving away their passwords in order to gain access to network.

**Risk 3**: Nation-states might try to steal intellectual property of the education institutions. This is mainly research work.

**Risk 4**: Nation-states might try to steal the PII about the students and staff to leverage it in forcing them into unethical practices, espionage etc.

**Risk 5**: Nation-states might try to utilize the computational power associated with the educational institutes to carry out DDoS attacks against enemy states.

### Cyber-Criminals

**Risk 1**: Cyber-criminals might try to obfuscate their digital footprint and avoid attribution.

**Risk 2**: Cyber-criminals trick the genuine users in giving away their passwords in order to gain access to network.

**Risk 3**: Cyber-criminals might try to steal intellectual property of the education institutions. This is mainly research work.

**Risk 4**: Cyber-criminals might try to steal the PII about the students and staff to sell it on illegal platforms like Dark-web.

**Risk 5**: Cyber-criminals might try to inject false information in the student administration or LMS systems (like false grades, credits etc.) for monetary gains.

**Risk 6**: Cyber-criminals might try to utilize the computational power associated with the educational institutes to carry out DDoS attacks against warranted entities and for crypto mining.

**Risk 7**: Cyber-criminals might get paid from the competitors to deface their opponents or tarnish their image for business gains by sabotaging the customer facing interfaces.

### Hacktivists

**Risk 1**: Hacktivists might sabotage the financial well-being indirectly by attacking a school and creating a bad reputation for them.

**Risk 2**: Hacktivist might attack a school to prove their point or as a sign of protest against that institution (against raging matters like expensive education, institutions stand on certain matters, etc.)

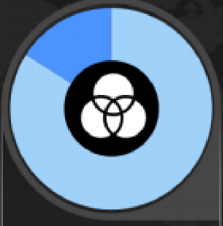
### Students

**Risk 1**: Students might Risk 1: Students might sabotage the reputation of the school reputation as an act of retaliation or to prove a point.

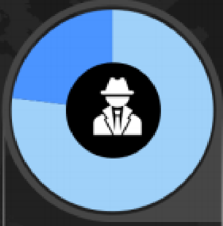
**Risk 2**: Students might try to gain unauthorized access to the student administration systems & change their grades, credits etc.). sabotage the reputation of the school reputation as an act of retaliation or to prove a point.

## Areas of Improvement

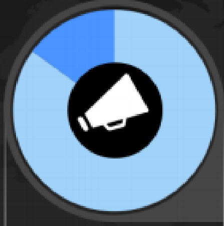
*(Based on the threat landscape for Education sector)*



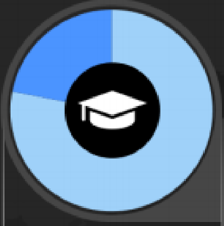
16%
Nation-states
Skill: high
Resource: full
Will: high
Motive: nationalistic



23%
Cyber-criminals
Skill: medium-high
Resource: medium-full
Will: medium-high
Motive: monetary



15%
Hacktivists
Skill: low-medium
Resource: low-medium
Will: medium-high
Motive: social



22%
Students
Skill: medium-high
Resource: low
Will: low
Motive: learning or amusement

## Positives

- A pre-defined information Security policy
- A function SOC / IRT function
- Executive management familiar with the risk appetite of the institution
- User awareness trainings
- Full compliance with Data Privacy laws like GDPR
- Pre-defined BCP / DR plans in place
- Dynamic Intrusion prevention Controls
- Clear overview over all Information assets.

## Areas of improvement

- Lack of overview on all IT Assets (Asset management)
- Lack of measures to verify the effects of user awareness trainings
- Lack of vetting processes prior to employment of key personnel
- Lack of resilience testing of the Disaster recovery controls
- No defined mechanism for data classification
- Lack of measures like secure printing to ensure confidentiality of information.

# Recommendations

## (Based on ISO /IEC 27001 standard)

### Policies

- Use of an *Asset Management* system can assist in better overview of threats and risks.
- Consider acquiring a dedicated function like a Chief Information Security Officer (CISO) and/or Data Privacy Officer (DPO) to assist with information security management in your organization.
- Consider allocating dedicated annual budget towards information security efforts and an emergency fund, should there be a security incident and needs urgent mitigation.
- Consider implementing a strict BYOD policy to ensure that infected devices are not introduced to your network.
- Consider conducting self-benchmarking via internal or external IT Audits annually. It can assist in better panning and efficient resource allocation towards risk management.
- Consider conducting exercises to check the maturity of IT users against phishing or social engineering attacks.
- Consider conducting DR drills to see the efficacy of the Business Continuity & Disaster Recovery Plans periodically.
- conducting a DPIA on all your information collection, processing and storing systems to ensure regulatory compliance.
- Consider making a BCP / DR plan to ensure continuity of operations and ensure availability which is mission critical in education sector.

### Storage

- Consider instating access controls on any place where your IT Infrastructure equipment is stored to ensure authorized access with logs (accountability).
- Consider adopting md5 security solutions on workstations where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.

### Applications

- Consider develop routines to check if all the accounts are terminated when not needed anymore – for employees, guests, vendors, consultants, etc.
- Consider developing a patch management routine or a workflow to install them periodically and also on emergency basis – automatic update installation on mission non-critical applications.

### Network

- Consider MAC tagging on the switch ports to avoid spoofing for business-critical functions like HR, CFO, CEO, etc.
- Consider enabling 802.1x (or similar protocols) on the switch port so that even if somebody gains unauthorized access to the building, he will still need to authenticate to access internet.
- Network segmentation and firewalls rules to restrict communication horizontally can help in restricting the attack surface (across VLANs).

### Servers

- Consider adopting md5 security solutions on servers where only approved files can run in your environment. This blocks remote injection and execution of malicious payload.
- Endpoint protection or strict firewall rules with real time alerts, should there be an intrusion or even an attempt.

### Information Management

- Consider structuring your data on a department level (on three levels – public, shared and private) that will give you a better insight into your data assets and appropriate access controls can be instated subsequently.
- Consider adopting a clear-desk policy to ensure that unauthorized individuals don't get access to confidential information. Controls like secure printing can assist.

18476( 1)
18437( 1)
-68
-92
4th
18594 ( 1)
18589 ( 4)
18590 ( 1)
18567 ( 2)
18567 ( 9)
18560 ( 5)
18514 ( 1)
18390 ( 1)
tically updated during trad
18440
18357
Bid (Qty)
Ask (Qty)
18590( 2)
18591( 1)
18588( 1)
-60
-70
-0.32
-0.37

**Maritime Corp.**

*Q4, 2019*

SECURITY | SCORE

BY IVAN@NTNU

Issued by **Ivan Talwar**

*MIS, NTNU (Gjøvik)*

SECURITY | SCORE
BY IVAN@NTNU

NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Summary Report

## Provided to

*Maritime Corp.*

## Issuer (on behalf of NTNU)

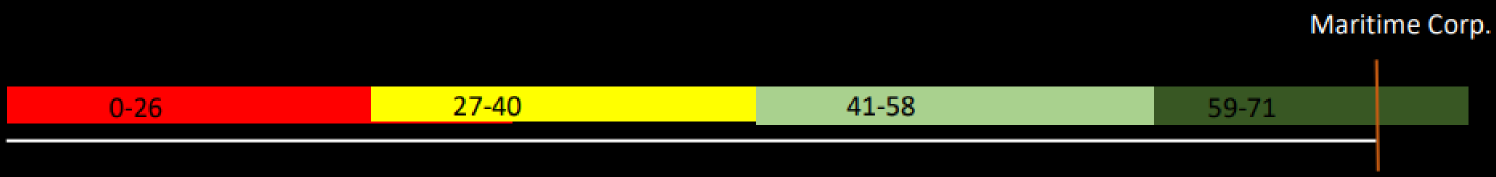
Ivan Talwar

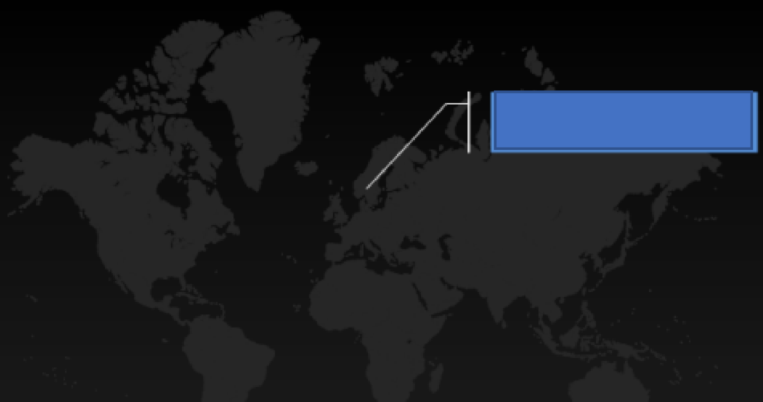
## Date

December 05, 2019

## Your estimated score is

**65***

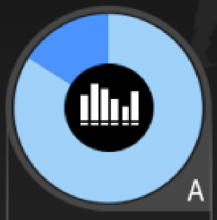




## Areas of Improvement

3%

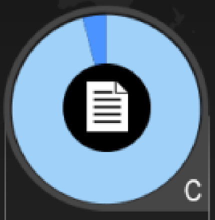
Your security posture is very good. It is very important to maintain and further improve it since the threat landscape evolves constantly. In the next sections, we will recommend some mitigation steps that you might find relevant.



16%

Networks

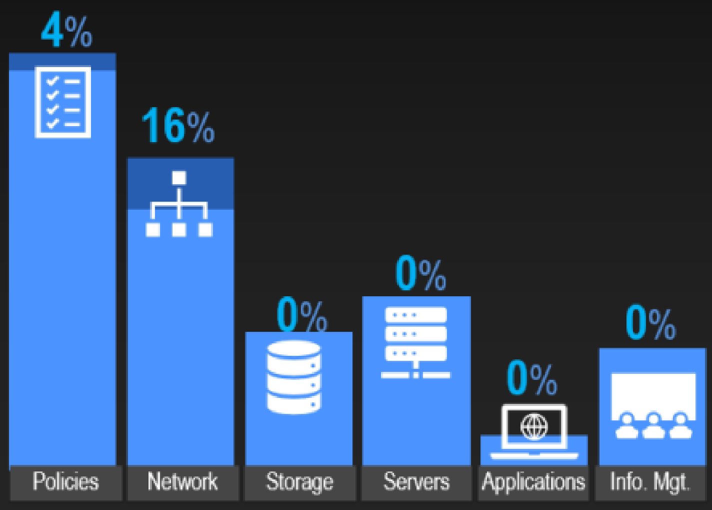
- IP/User tagging with 802.1x
- Port level authentication
- MPLS for real time data integrity



4%

Policies

- Time bound guest WIFI access to the network



Copyright@2019 – SecurityScore by Ivan Talwar

SECURITY | SCORE
BY IVAN@NTNU

For:
Department of InfoSec & Comm. Tech.,
NTNU, Teknologivegen 22 ,
2815 Gjøvik

# Threat Landscape Report
## (Sector based)

15%

## Threat agent based exposure

This is [redacted] threat exposure score. This is based on the sector-specific risks. Some of the relevant risks have been mentioned that are applicable to the entire maritime sector.

**Typical assets for Maritime Sector**

- *Automated Identification Systems* for vessel identification
- *Radar* for Radio detection and ranging
- *GPS* for global position fixing data
- Communication systems on board
- On deck machinery
- *Cargo Management System* for live tracking of cargo

### Nation-states

**Risk 1**: Nation-states might acquire intelligence on vessel movement in disputed waters or areas of high strategic value.

**Risk 2**: Nation-states might use disruptive techniques to de-route the vessel by spoofing real navigation signals.

**Risk 3**: Nation-states might target the intellectual property, commercial details, defense plans and personal data about people in key positions.

**Risk 4**: Nation states might target the communications of a vessel to snoop onto the energy untapped reserves in the area.

**Risk 5**: Nation-states might cause disruption by infecting the CNC machines (thus SCADA devices) like in case of Stuxnet.

### Cyber-Criminals

**Risk 1**: Cyber-criminals might acquire positioning data about the vessels and sell it further to the pirates.

**Risk 2**: Cyber-criminals might launch a ransomware attack on the systems aboard the vessels which can leave the vessel stranded in the middle of nowhere in the absence of onboard navigation and communication systems.

**Risk 3**: Cyber-criminals might disrupt the cargo tracking function onboard, thus disrupting the supply chain management of the associated companies.

**Risk 4:** GPS signals can be spoofed and the autonomous vessels can be guided to the pirates' desired destination.

vector or a backdoor to main target's network, as happened in the case of Stuxnet

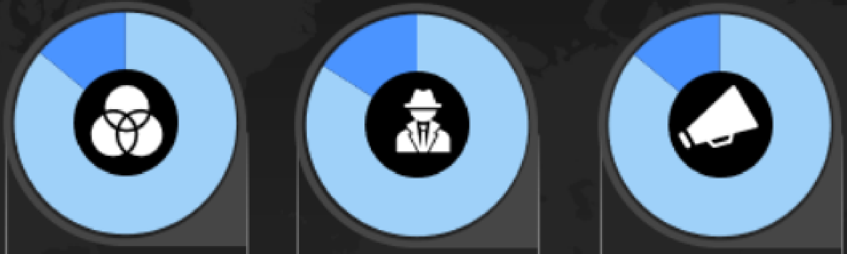
### Hacktivists

**Risk 1**: Hacktivists might cause disruption to show their protest against climate change, whaling issues, and environmental issues.

**Risk 2**: Hacktivists might deface the shipping company by taking control of the customer-facing interfaces and post messages in accordance to their agenda.

## Areas of Improvement

(*Based on the threat landscape for Energy sector*)



14%
Nation-states
Skill: high
Resource: full
Will: high
Motive: nationalistic

16%
Cyber-criminals
Skill: medium-high
Resource: medium-full
Will: medium-high
Motive: monetary

14%
Hacktivists
Skill: low-medium
Resource: low-medium
Will: medium-high
Motive: social

### Positives

- A pre-defined information Security policy
- Network segmentation for optimization of data traffic security
- Dynamic Intrusion Prevention controls
- Redundancy on storage to ensure availability
- Physical security controls on datacenter
- Encrypted drives to mitigate theft incidents
- File level (hashing) security for explicit approval for execution of a file
- Segregation of regular user accounts and administrator accounts
- Patch Management

### Areas of improvement

- While generating guest accounts, consider making them timebound so that they cannot be re-used and misused.
- Consider enabling 802.1x (or similar protocols) on the switch port so that even if somebody gains unauthorized access to the building, he will still need to authenticate to access internet.
- Consider adopting services like MPLS for functions that require real time data to ensure data integrity.

18476( 1)
18437( 1)
4th
5th
18594 ( 1)
18589 ( 4)
18590 ( 1)
18567 ( 2)
18567 ( 9)
18560 ( 5)
18514 ( 1)
18390 ( 1)
tically updated during trad
18440
18357
Bid (Qty)
Ask (Qty)
18590( 2)
18591( 1)
18588( 1)
-60
-70
-68
-92
-0.36%
-0.50%