Transformation of Cybersecurity Posture in IT Telecommunication: A Case Study of a Telecom Operator

Ahmed Adel[1*], Dilshad Sarwar[2], Amin Hosseinian-Far [2]
[1] University of Northampton, and Ericsson, ahmed.adel@ericsson.com
[2, 3] University of Northampton, {dilshad.sarwar, amin.hosseinian-far}@northampton.ac.uk

ABSTRACT

Organisations are facing sophisticated and advanced persistent threats (APT) that are targeting sensitive information assets. Any form of cyber-presence can be typically attacked by adversaries, and the motives of such attacks are context dependent. Besides, users and organisations are prone to software vulnerabilities, mis-configurations, outdated systems and several other systemic defi-ciencies which can be leveraged to compromise enterprise assets and gain an initial foothold within an organisation network. The aim of the paper is to develop a flexible and generally comprehensive organisational strategy to defend against the massive increase in cyberattacks, in order to protect the strategic business objectives of an organisation and keep an alignment between business objec-tives and security. Moreover, this paper reflects on the work under-taken by multiple teams within the chosen case study organisation to enhance the cybersecurity.

KEYWORDS

Cybersecurity, Security Operation Centre, Cyberculture, IT Telecommunication, Cyber Resilience

1. INTRODUCTION

Cyber Security, a term that is used a lot nowadays. In an era of information and communication technology (ICT), the value of the data is very crucial, especially when it comes to personal information, credit cards information, or financial information. Today everything is moving through the Internet, all aspects of the business operations pass through the Internet. On this basis it is therefore imperative that the IT infrastructures are secure.

Cybersecurity is a culture that must be introduced to everyone to increase awareness and reduce negative impacts on organisational information and data security. No hacker will spend time and effort to hack any system that contains no information or invaluable information. Therefore, understandably sectors such as telecommunications and banking are under attack by cyber criminals on an ongoing basis. Recent reports indicate 43% of telecommunication organisations suffered a DNS-malware attack (InformationAge, 2018). Moreover, the top five cybercrime attacks were Phishing scams, Identity Theft scams, Online Harassment, Cyberstalking and Invasion of privacy (SpidyMan, 2020). This paper will talk about cybersecurity in the area of telecommunications, and look at the importance of the security department within organisations, focusing on how to spread the value of cybersecurity to reach a state where all employees in the organisation support cybersecurity. A case study will be conducted in the area of telecommunications, in the region of the Middle East and Africa. It was challenging to know

where the organisation under the study is on the cybersecurity posture spectrum. Unfortunately, after severe incidents and significant compromise attempts, the organisation obtained management commitment and support for the new security strategy and program. Security can't start from the middle of the organisation. Ultimately, to achieve significant improvement in information security, senior management and the board of directors must be held accountable for information security governance. They must provide the necessary leadership, organisational structures, oversight, resources and processes to ensure that information security governance is an integral and transparent part of enterprise governance.

2. LITERATURE REVIEW

Cyber-Security became an important area to consider for any organisation running its business on networks or the Internet. So, security awareness became essential for all employees working in all areas. The process of saving valuable information became the responsibility for everyone to undertake. The security department has the upper hand to make sure the organisations processes are in place, regarding tools, and procedures, but the implementation and respect to the process will remain the success factor. For any organisation to move from the ignorance to the awareness, the organisations are required to follow specific steps for that. (Gundu and Flowerday, 2013; Rhodes et al., 2019, Safa et al., 2019) seek to disseminate information security awareness process that aims to cultivate positive security behaviours. To reach that they found that using either behavioural intention model based on the Theory of Reasoned Action, or the Protection Motivation Theory and the

Behaviourism Theory are imperative. They refined both the process and the model. This was then tested through action research and it was found that whether the organisation have or even implement an information security policy, this does not guarantee employees will understand their role in the organisation using security processes and save information assets. They also found that it is critical to design an information security awareness campaign to ensure objectives and requirements.

Bada et al. (2019) reviewed current information on security- awareness campaigns and the effectiveness of these campaigns on employees. They then examined the factors responsible for the change in online behaviour, such as personal, social and environmental factors. And, they finally summarised the most critical components for a successful cybersecurity awareness campaign, also, furthermore factors were also examined which could lead to a campaign's failure.

de Bruijn and Janssen (2017) indicates that society is turning into a cyber-physical community entirely depending on Information and Communication Technology (ICT) due to the rapid change in the digital life we are living. In return, this makes the need for cybersecurity is a must.

Limba et al. (2017) elaborate that for critical infrastructure that uses technologies based on communication and information technology, it depends on cybersecurity. Organisations are trying to make themselves safer from vulnerabilities. They provided theoretical aspects that can be used to ensure security on the critical infrastructure. The cybersecurity model is analysed from management perspectives

and is not concerned with technological issues. They also explained that the private sector is much less inclined to share information about specific attacks, although such information could suggestively contribute to the field of cybersecurity. The model consists of six core sections.

Figure 1: Cyber Security Model Source: Limba et al. (2017)

Limba et al. (2017) have defined the security levels from initial, medium and the highest level of the cybersecurity management model, which they call it interoperability level, which characterised by the full interconnection of all management model dimensions. They indicate that on this level, the organisation is operating as a vast army

of soldiers and the cybersecurity model is an inherent part of the organisation which is in line with De Bruijn and Janssen (2017).

Nowadays, when the threats are rapidly disseminating everywhere, Organisations needs to evolve solutions that have more complex measures. As cybersecurity management model considering all strategic aspects.

Sallos et al. (2019) Agree on the last point of Limba et al. (2017) that Organisations must consider cybersecurity through a strategic lens. It must be as a function that must be adopted by everyone. They find that Cybersecurity management is not straight forward, as it is a culture and not a task. It also requires focused consideration in terms of strategies, structures and practices. Sallos et al. have set out the basis holistic view of knowledge which focus on action-results. Sallos et al. also highlighted the importance of a knowledge-based approach to be taught as a concept for the employees.

Von Solms and von Solms (2018) highlighted that higher management must clearly understand the cybersecurity, and it's the security department task to make it clear for them to ensure the more senior management buy-in. They succeeded to define the relationship between cybersecurity and information security, concerning the governance perspective. By this, they were able to ensure the board of directors by in, for investment. Moreover, understanding of what cybersecurity cause to the business can if it is absent. They succeeded to make a clearly state that the Cybersecurity target is to protect the organisation against the risks that may harm the business as a whole. The more the organisation is dependent on the Internet, the higher the cyber threat.

Paul et al. (2018) state that to enhance cybersecurity, the organisation must study first what is cybersecurity and what are the risks that may occur. They suggest that every organisation should do the following

- Learning about the basics of Computer and Cyber related terms and concepts.
- Learning about the basics of Security related concepts such as (Computer Security, Network Security, Database, Web Security, IT Security).
- Learning about Information Security and Information Assurance.
- Learning about the fundamental characteristics of Information Assurance.
- Learning about the Function and Role of Information Assurance in general.
- Learning about the laws governing IT and Cyberworld.
- Learn about expressions (Table 1)

Cyber café	Cybercrime	Cybernetics	Cyberspace
Cyber hygiene	Cyberwarfare	Cyber organism	Cyberlaw

Cyberattack	Cyberculture	Cyberage	Cyber forensic

Table 1: Cybersecurity Expressions adapted from Paul et al. (2018)

Paul et al. (2018) also recommend that each organisation at least must have one of the following functions if not all when it comes to huge organisations with valuable information system in place.

Cybersecurity analyst	Cybersecurity expert	IT Manager	IT security analyst
Cyber forensic expert	Ethical hacker	Data security analyst	Web security analyst

Table 2: Cyber Security Functions adapted from Paul et al. (2018)

Al-Mohannadi et al. (2018) clarify the threat of cybersecurity threats among IT employees. within this, it has been highlighted that a Cyber-attack is one of the critical issues for most of the organisations. Organisations and Governments are doing their best to protect valuable data from being stolen. There are many systems such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), firewall, packet shaping devices which are available to protect networks. There are also attack modelling techniques that organisation can perform patterns from them to understand the nature of the attack. Thus today, most of the organisations have a security operation centre (SoC) to be the first and most solid layer to protest the organisation from cyber-attacks. They concluded that employees must have awareness sessions and learn about cybersecurity, and this is in line with Bada t al. (2019). They also highlighted that IT

employees need to improve their knowledge about cyber threat. It was also found that there is a gap of understanding between Security operation team and other IT experts. SoC team are generally capability of safeguarding from cybersecurity threats if they can identify it. Kirkas et al. (2019) highlighted the importance of Security operation center as a central level responsible for monitoring, analysing, assessing and defending the organisation asset. This is the most important department under any IT infrastructure domain.

Vukašinović (2018) highlighted that each organisation must have cybersecurity measures. In the field of telecommunication, he found that according to research, mobile phone users are increasingly exposed to cyber-attacks. After analysing more than 400 000 applications available in the most popular apps and Google applications, it was found that 14 000, or 3% have security vulnerabilities, including sensitive information such as location, text messages and contacts. He discovered that Cybersecurity attacks are divided into two groups; the first group is the passive and the second group involves active attacks. In the passive aggression, the attacker gets rights without changing the content of messages. In the active attacks, the attacker can modify, delete, copy the contents of files, set himself as an authorised user, disable functions and do whatever he wants. The protection of any network systems should follow the following:

- Confidentiality
- Integrity
- Availability

Vukašinović agrees with most of the above articles that there is no fully protected computer network. The most secure system is one that is not connected to the Internet at all. The protection given to the network systems is a must nowadays. And, by ensuring protection, Organisations will enable preventing unauthorised intrusion. Monitoring systems need to be used to reduce the security risks of intervention into systems.

Vähäkainu and Lehto (2019) highlighted the importance of artificial intelligence (AI) to help cybersecurity management. They indicate that organisations benefit from the ability of (AI) systems to improve their expertise quickly and from sharing it to all those who need it. They discussed the following cybersecurity areas:

Infrastructure security	Endpoint security	Application security	IoT-security
Web-security	Security operations and incident response	Threat intelligence	Mobile security
Cloud security	Identity and access management	Network security	Human security

Table 3: Cybersecurity areas adapted from Vähäkainu and Lehto (2019)

Their study highlighted that information on 11 artificial intelligence solutions were gathered. These perspectives were divided into the following areas:

- infrastructure security
- endpoint security
- web security
- security operations and incident response
- threat intelligence, mobile security and human security

Vähäkainu and Lehto (2019) have concluded that the (AI) system should detect and quickly react to any attack, such as an abnormal login, and/or suspicious usage of cloud services. There are many ways to detect threats. But, as an organisation may face up to 200000 information security events per day the investigation of the threats by using human information security specialists is expensive and is time-consuming, and therefore (AI) is a must nowadays.

3. METHODOLOGY

The methodology used in this paper is the Design Science Research Methodology. Binandu (2016) explained Design Science as it is concerned with knowledge acquisition that relates to designs and activity which offer a specific guide to for evaluation and iteration within a project. While research methodology is also seen as an action plan, strategy, process, behind the choice of and methods and linking the choice of methods use (Alturki et al., 2013; Binandu, 2016). Design Science Research Methodology (DSR) is considered to be the other side of Information System research that evaluates information Technology artefacts needed to solve problems identified in an organisation.

Design science research contributes highly in the field of Information Systems as it measures the way it is applied to business needs. It solves an existing problem. Therefore, there is considered to be one of the most useful methodologies in these fields (Hevner et al., 2004; Binandu, 2016; Peffers et al., 2018).

This methodology is that it is used when there is crucial dependence upon human cognitive abilities to produce effective solutions. Or personal social skills are a critical dependence upon to deliver effective solutions which is the case in this paper and the case study too (Gleasurea, 2015; D. Binandu, 2016; Bisandu et al. 2018).

The Design Science Research Methodology has found to be an excellent method in the Information Science and Computer Science because it is a method that works with human, organisational social kind of problem-solving through artefact development (Hevner et al., 2004; Binandu, 2016).

4. CASE STUDY

1. Understanding the cybersecurity posture

The security status of your enterprise's software and hardware, networks, services, and information; your ability to manage your defences; and your ability to react to and recover from security events are collectively referred to as your cybersecurity posture. Understanding and defining the full scope of your cybersecurity posture is essential to protecting your business against breaches (Balbix, 2020).

To understand and optimise your cybersecurity posture, you need to:

- Analyse what it currently looks like
- Identify the possible gaps
- Then take action to eliminate those gaps

"The thing that kept me awake at night (as NATO military commander) was cybersecurity. Cybersecurity proceeds from the highest levels of our national interest ... through our medical, our educational, to our personal finance (systems)." Admiral James Stavridis, Ret. Former-NATO Commander (Gartner, 2020)

Unfortunately, most people do not understand the gravity of the problem until it personally affects them through identity theft or other malicious activity. Unsurprisingly, however, the rate of cybersecurity-related crime is exploding, and a recent study claims that there is a new victim of identity theft every 2 seconds in the United States alone (SelfKey, 2020).

On top of that, Half of the cyberattacks are targeting small businesses that usually don't have sufficient cybersecurity to protect themselves from such threats. In a Statista report in 2018, the most notorious cyber-attacks experienced by companies of all sizes include phishing (37%), network intrusion (30%), inadvertent disclosure (12%), stolen/lost device or records (10%), and system misconfiguration (4%) (Statista, 2020).

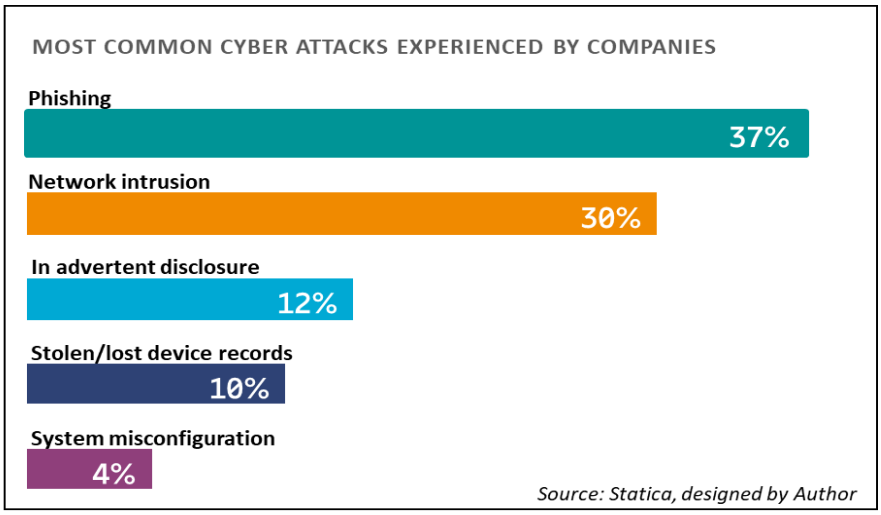

Figure 2 Most common cyber-attacks, Source: Statica (2020)

1.1 The Turning Point

Understanding the current security posture and identifying gaps in existing organisational security systems is very important. It will require skilled resources and tools, audits- both internal and external are one of the main processes used to determine information security deficiencies from control and compliance standpoint and are one of the essential resources in strategy development. Early detection of security problems and solving it will be a cost-effective solution for developing secure systems (Yu et al., 2017).

The turning point had started when there was a successful attempt to attack one of the mission-critical systems and investigations found that the system was compromised. The attacker targeted confidential information assets. Fortunately, the effort failed due to unexpected server behaviour, and the attacker zipped the theft data in the same server, causing service interruption due to file system

utilisation. On top of that, this incident reported a service availability issue. This is considered as cybercrime (Jahankhani, 2014)

1.2 Gap Analysis is the base for Strategy development

In addition to the costs that companies face to deal with the immediate effects of an incident, security incidents can cause more costly, long-term harm such as damage to reputation and brand. Beyond the impact to market capitalisation, if the issue threatens the public good, regulators may intervene, enacting stricter requirements to govern future business practices. "Data breaches stain the reputations of companies both big and small, damaging the brand and reducing consumer trust, and sometimes the consequences can affect the company for years to come," (T. Seals, 2017) notes Paul Bischoff, researcher and privacy advocate at Comparitech.

In our case and after the security incident; the response and actions of management were hugely influential; their support helps to develop the implementation of the remediation strategy. According to Kaspersky Lap detection data; we found that a sizeable Iraqi telecom provider was deeply compromised with 10% of their endpoints infected with POWERSTATS

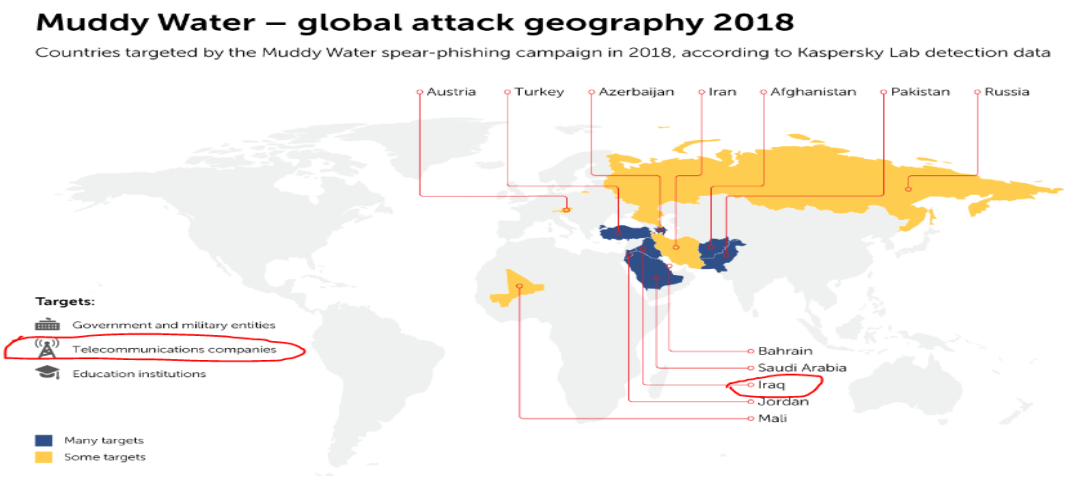

Figure 3 Source: Kaspersky (2018)

As with any complex problem, a lot of questions need to be answered to identify where you are:

- Do we have a real-time inventory of all our assets, asset calcification?
- Are we able to continuously monitor our assets?
- Do we have security incident management in place?
- Do we have a backup process, DR, and BCP?
- Do we have security metrics?

Gap analysis (Crumpler, W. and Lewis, J.A., 2019) identified 39 Security gaps and deviations in security tools, processes, execution and management system. End of service, End of life (EOS/EOL) operating system are still in the operation state, hardening, patch management and user access management are not defined. Security policy, regulatory standard and governance, risk management are not defined; some systems were compromised already.

The gaps between the current stat and desired stat paved the way to develop the security strategy and developing the road map to achieve the objectives. The desired defined based on the outcomes set by management, regulatory requirement and a variety of frameworks to ensure defence in depth.

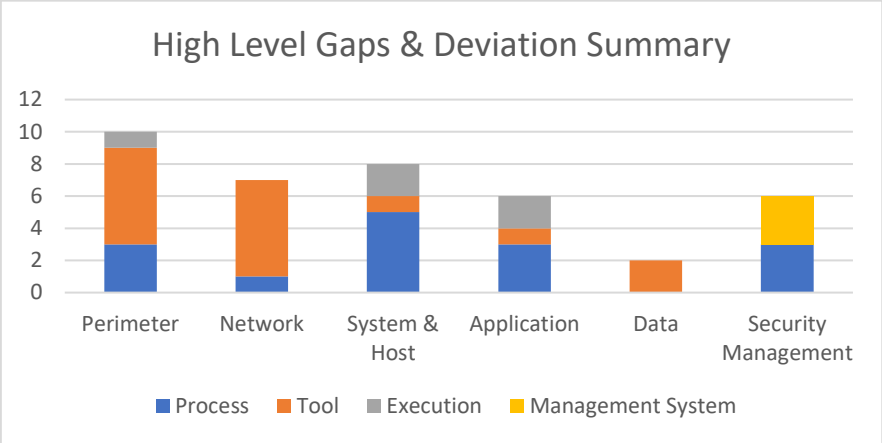

Figure 4: Gaps and deviation summary (graph developed by Authors from real organisation data)

The full security audit was finalised after the major security breach, below are the summary of the gaps identified:

- VPN Users gain access directly, Multi-factor authentication is missing, VPN user time out is not in place.
- Anti-Spam and Anti-Virus implemented; the effectiveness of the tool usages not measured.
- The absence of log management and the centralised log management solution available for the network.
- No real-time security attributes monitoring of the devices and nodes except bandwidth monitoring.

- No distributed denial-of-service (DDOS) protection implemented.
- No Advance Threat protection.
- Terminal Access Controller Access Control System (TACACS) is not implemented for all network devices.
- Zone segregation is not defined.
- No Next-Gen firewall available, current firewall policy is based access-list only. Ext to int for any to an internal subnet is allowed, many test rules also presented, No FW rule validation in place.
- Antivirus management servers are exposed with full Internet access, same control to be validated on other servers.
- Network Segmentation for Management & data is not implemented for all.
- Vendor allowed to connect the corporate network with their device. No control over for third party / non-standard systems to connect thus causing vulnerable.
- Asset management tracker in place, however no EOS / EOL details for the devices and tools are highlighted. The tracker is not updated regularly.
- No defined hardening processes. Antivirus & Vulnerability status are verified during the commissioning process.
- Undefined patch management process in place. Patch management is followed on reactive / OnDemand manner and no zero-day patch management process, still many critical patches are in an open state, and many EOS / EOL systems are running in the infrastructure.

- Vulnerability scan performed for critical system only, the mitigation process is not well defined and not aligned with GRC; even some critical vulnerabilities are still open.
- No IDM tool in place, No ID & access revalidation in place and No password age and password reuse policy implemented.
- All the clients not configured to route through a proxy.
- Clear text services are like telnet, FTP, HTTP is allowed from outside.
- No defined policy in place.
- Only a few components have the process documents and no procedure or SOP available.
- No defined metrics for all the Security measures.
- There is limited security governance in place; Security governance is not aligned with the Org level. Elevation/escalation of compliance & security weakness requires leadership decision.
- Business continuity plan (BCP) and Disaster Recovery (DR) process are not in place, No BCP / DR test executed. Only critical systems data backup is happening and stored in DR locations.

1.3 Road Map for Remediation

An implementation plan was formalised as a road map to close all tactical and strategic gaps (Kapur, 2017). The Implementation plan started immediately after the assessment conclusion. The business case developed for investment in security tools and controls. Prioritising action items and addressing the most critical vulnerabilities

and issues first guide the roadmap of our entire defence strategy and influence our security spending.

To improve and raise your Cybersecurity posture and awareness, you don't need to invest endlessly in new security tools. The truth is that 80% of data breaches can be prevented with necessary actions, such as vulnerability assessments, patching, and proper configurations. An example is Phishing attacks are the most common cybersecurity attack. This type of attacks is a big part of why there are so many compromised passwords. In the last year, 76% of businesses reported that they had been a victim of a phishing attack (Info Security, 2017), security awareness is the most effective control to mitigate the risk of phishing attaches (Staff, 2017).

In addition to the immediate response to isolate the compromised system and the eradication effort, the Tactical (6 months) and strategic (3 years) action plan formalised, and our security program started immediately with ultimate commitment from C-level management to ensure the required resources.

1.4 Actions were taken to eliminate the gaps

The steps taken consist of controls, processes, and practices to increase the resilience of the computing environment and ensure that risks are known and handled effectively. These activities dealt with by an internal team supported by external vendors as needed.

1.4.1 Security enhancements in the Security Tools

Although cybersecurity spans technical, operational and managerial domains, a significant portion of the actual implementation of the information security program is likely to be technical (Weir, C. et al., 2019) below are the summary of the security enhancements in the security tools;

- SEIM tool is currently used by the security team and SOC for log monitoring and security management.
- Multi-factor authentication is currently used for VPN, Webmail and servers' access.
- Network (LAN and Wireless) security controls have been implemented based on least privilege using Cisco ISE.
- Enterprise password management tool used for local admin control.
- Windows and Linux security patching tools are currently used for centralised patch management.
- Advanced Threat Protection ATP is used.
- Next-generation firewalls are used in the network.
- Next-generation Antivirus is used in all clients and servers.
- New proxy servers.

1.4.2 Security enhancements in Process and Governance

Process and governance must be an integral and transparent part of enterprise governance and complement or encompass the IT governance framework (Ávila, C. et al., 2019). Integrated with the processes they have in place to govern other critical organisational resources. It includes monitoring and reporting processes to ensure

that governance processes are effective and compliance enforcement is sufficient to reduce risk to acceptable levels. below is the summary of the security enhancements in process and governance;

- User Access management process
- Security Patch management process
- Vulnerability management process
- Log management process
- Antivirus management process
- IT security Weekly meeting to discuss security operations and project.
- IT security reports and metrics (KPIs and KRIs)

on top of the governance and processes enhancements, all security policies reviewed and updated with management intent.

1.4.3 Security enhancements in IT operations

Poor configuration in IT operations can lead to cyber criminals bypassing internal policies that protect sensitive information. Setting security baselines for an organisation's operational enterprise has several benefits. It standardises the minimum amount of security measures that must be employed throughout the organisation; this results in positive benefits for risk management. It also provides a convenient point of reference to measure changes to security and identify corresponding effects on risk. A lot of security enhancements has been achieved in IT operations;

- IT severs, and Client PC is full patches with the latest security updates,

- Next-generation antivirus has been installed in all client PCs and servers and monitored,
- Close all discovered critical vulnerabilities within SLA time-line,
- Physical access control to datacentres is managed and integrated with an access management tool
- Data uploading is monitored 24X7 by NOC.
- Enhancement in security incident handling,
- Upgrade or Isolate EOL/ EOS systems.

In addition to all this security enhancement, new SOC function has been established to monitor security attributes for IT assets 24/7 and analysing logs and respond to a security incident to increase speed and agility in security. Preparing the workforce to protect their environments is vita.! As much as it is essential to have in place all security measures to safeguard the information systems infrastructures, hardware and software alone cannot withstand the attacks of malicious staff training, and security awareness is critical security control.

2. Current Cybersecurity Posture; Today Vs Past

The quick fix actions and short-term tactical plan are practical and affordable ways to reduce the exposure and avoid the worst to happen. The overall security program has a significant impact on information security readiness and on the capability of the staff to deter potential attackers.

Now, our enterprise has documented all of its programs and procedures, and it has a clear understanding of its risk. It is not the

endpoint, in addition to strong KPIs and KRIs, continues assessment, testing and audit is an essential part for continues improvement in the cybersecurity posture and ensures the security control effectiveness.

The enterprise ranked No.1 in cybersecurity posture by group risk management. Furthermore, the last security audit and penetration test report a considerable enhancement in cybersecurity capability.

A lot of security dashboards and security automation developed by a security team internally, KPIs and security metrics reflect strong security governance and risk management. Continuous monitoring for security events, incident detection, identification, handling, post-incident review and security awareness increased our ability to react to and recover from security events. Organisation 24/7 SOC increased the velocity of security event handling and detection for the intrusive/malicious/suspicious/misconfiguration/policy violation etc. events before getting a serious issue.

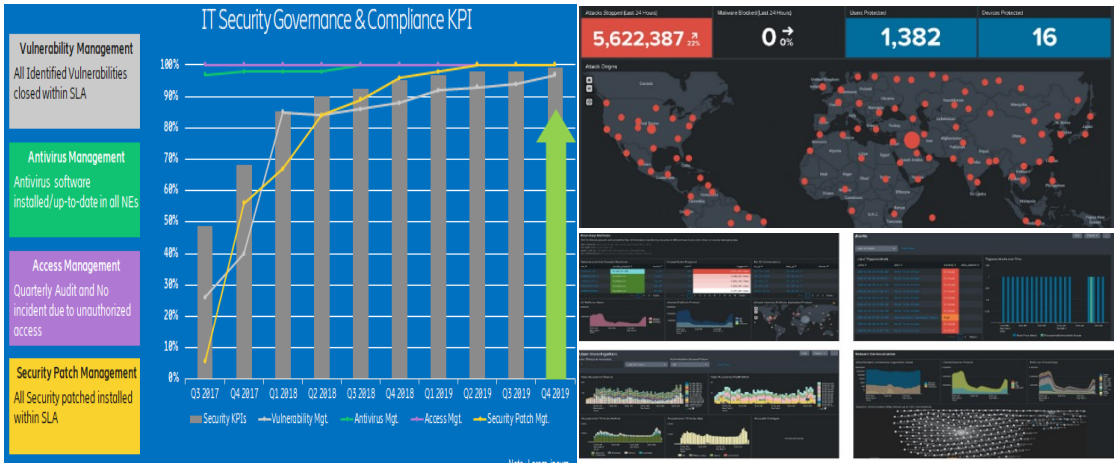

Figure 5: Security Governance & tools (Organisation own developed tools)

Staff training and awareness sessions enhanced cybersecurity culture in our organisation, and this is reflected by the increased number of a reported security incident. Developing the technical staff take their skills to the next level that can be used in penetration testing and threat hunting.

3. Conclusions and Recommendations

The security status of the enterprise's assets, ability to manage defences, and the ability to react to and recover from security events are the most useful indicators for cybersecurity posture.

An organisation transformation plan, along with the best practices that have been followed, helped building a cyber-resilience strategy and improve the security posture of any organisation. It is essential to create a culture of security awareness across the organisation and among employees. This is the best way to provide a constant barrier that deters cyberattacks that take advantage of human behaviour.

A severe breach can result in data loss or potential damage to the IT infrastructure and have adverse effects on essential company operations and on the business itself through the loss of confidentiality, integrity or availability of informational assets.

Any security transformation program requires, of course, the strong commitment, direct involvement and ongoing support from senior leaders/executives. Such efforts are constant and permanent, which

therefore require continuous evaluation, funding and support. Inconsistency will cancel out any steps forward and opens the organisation to increased risks.

Defending against sophisticated threats ultimately requires mature processes and competent, dedicated security professionals. Sophisticated attaches require a thoughtful process that can prevent, detect and respond to threats with speed and agility.

While cybercriminals represent a significant threat, in most cases, the critical threats to organisations are their lack of adequate defences and employees who are ignorant of cyber threats. Organisations can reduce their risks of cyber-attacks by following industry best practices and implementing key defence measures such as employee training and the use of encryption.

What cannot be measured cannot be managed. Security metrics and thresholds should be defined for specific control and process to measure the extent to which performance objectives are being achieved on an ongoing basis. Security status trends reports that are systematic and timely are a useful tool to maintain management commitment and support. Organisations had to start implementing the culture of security to their employees. Security awareness also had to be disseminated across the organisation to make sure that everyone is aligned and knows the importance of security. One of the key strategies in security is “No exceptions” when comes to security and important information inside the organisation (Sennewald, C.A. and Baillie, C., 2020).

REFERENCES

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., Musa, A. (2018) Understanding awareness of cyber security threat among IT employees. *Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2018*. (August), 188–192.

Alturki, A., Gable, G. G., & Bandara, W. (2013). The design science research roadmap: in progress evaluation. *PACIS 2013 Proceedings*.

Ávila, C., Chinchilla, E.J., Velásquez Pérez, T. (2019) It governance model for state entities, as support for compliance with the information security and privacy component in the framework of the digital government policy. *Journal of Physics: Conference Series*. **1409**(1).

Bada, M., Sasse, A., Nurse, J. (2019) Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*. (July), 38.

Balbix (2020) Getting Started on Transforming Your Cybersecurity Posture. *Balbix*. [online]. Available from: https://www.balbix.com/app/uploads/eBook-Transforming-Security-Posture.pdf [Accessed March 23, 2020].

Bisandu, D.B. (2016) Design Science Research Methodology in Computer Science and Information Systems. *International Journal of Information Technology*. (November 2016), 1–7.

Bisandu, D. B., Prasad, R., & Liman, M. M. (2018). Clustering news articles using efficient similarity measure and N-grams. *International Journal of Knowledge Engineering and Data Mining*, **5**(4), 333- 348.

Crumpler, W., Lewis, J.A. (2019) The Cybersecurity Workforce Gap. *Center for Strategic and International Studies*. (CSIS), 1–10.

Demertzis, K., Tziritas, N., Kikiras, P., Sanchez, S.L., Iliadis, L. (2019) The Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks. *Big Data and Cognitive Computing*. **3**(1), 6.

de Bruijn, H., Janssen, M. (2017) Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*. **34**(1), 1–7.

Gartner (2020) Former NATO Commander Says Cybersecurity Most Worrying Threat We Face. *Gartner*. [online]. Available from: https://www.gartner.com/smarterwithgartner/former-nato-commander-says-cybersecurity-most-worrying-threat-we-face/ [Accessed March 23, 2020].

Gundu, T., Flowerday, S. V. (2013) Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*. **104**(2), 69–79.

Gleasurea, R. (2015). When is a problem a design science problem? *Systems, Signs & Actions*, **9**(1), 9–25.

Hevner R., A., Salvator T., Jinsoo Park, & Sudha Ram. (2004). Design Science in Information Science.

Ismail, N. (2018) Telcos struggling to mitigate the threats of cyber attacks. *InformationAge*. [online]. Available from:

https://www.information-age.com/telcos-cyber-attacks-123476699/ [Accessed March 23, 2020].

Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A. (2014) Cyber-crime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. pp. 149–164.

Kaspersky (2018) Middle-east focused threat actor Muddy Water extends attacks towards government targets in Asia, Europe and Africa. *Kaspersky*. [online]. Available from: https://www.kaspersky.com/about/press-releases/2018_muddy-water-final [Accessed July 1, 2020].

Kapur, R. (2017) Organization and Administration in Adult and Community Education. *International Journal of Information, Business and Management*. **9**(1), 141.

Limba, T., Plėta, T., Agafonov, K., Damkus, M. (2017) Cyber security management model for critical infrastructure. *The International Journal Entrepreneurship and Sustainability Issues*. **4**(4), 559–573.

Observer, C. (2020) 29 Must-know Cybersecurity Statistics for 2020. *Cyber Observer*. [online]. Available from: https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/ [Accessed March 23, 2020].

Paul, P., Bhuimali, A., Aithal, P.S., Rajesh, R. (2018) Cyber Security to Information Assurance: An Overview. *International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)*. (April), 1–9.

Peffers, K., Tuunanen, T., Niehaves, B. (2018) Design science research genres: introduction to the special issue on exemplars and

criteria for applicable design science research. *European Journal of Information Systems*. **27**(2), 129–139.

Rhodes, R.E., McEwan, D., Rebar, A.L. (2019) Theories of physical activity behaviour change: A history and synthesis of approaches. *Psychology of Sport and Exercise*. **42**(2019), 100–109.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T. (2015) Information security conscious care behaviour formation in organisations. *Computers and Security*. **53**, 65–78.

Sallos, M.P., Garcia-Perez, A., Bedford, D., Orlando, B. (2019) Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*. **20**(4), 581–597.

Staff, I. (2016) *CISM Review Manual - 15th edition*. Information Systems Audit and Control Association.

Statista (2020) Global No.1 Business Data Platform. *Statista*. [online]. Available from: https://www.statista.com [Accessed March 23, 2020].

SelfKey (2020) All Data Breaches in 2019 & 2020 – An Alarming Timeline. *SelfKey*. [online]. Available from: https://selfkey.org/data-breaches-in-2019/ [Accessed March 23, 2020].

Sennewald, C.A. and Baillie, C., 2020. *Effective security management*. Butterworth-Heinemann.

Seals, T. (2017) Post-Breach Share Prices Plummet Below NASDAQ Average. *Group, InfoSecurity*. [online]. Available from: https://www.infosecurity-magazine.com/news/share-prices-plummet-below-nasdaq/ [Accessed March 23, 2020].

SpideyMan (2020) Top 5 Popular Cybercrimes: How You Can Easily Prevent Them. *EnigmaSoft*. [online]. Available from: https://www.enigmasoftware.com/top-5-popular-cybercrimes-how-easily-prevent-them/ [Accessed March 9, 2020].

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K.K.R. (2019) A systematic literature review of blockchain cyber security. *Digital Communications and Networks*. (January), 1–10.

Vukašinović, M. (2018) Cyber Security Measures In Companies. *International Journal of Economics and Statistics*. **6**(September 2018), 125–128.

Vähäkainu, P., Lehto, M. (2019) Artificial intelligence in the cyber security environment. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*. (December), 431–440.

von Solms, B., von Solms, R. (2018) Cybersecurity and information security – what goes where? *Information and Computer Security*. **26**(1), 2–9.

Weir, C., Becker, I., Noble, J., Blair, L., Sasse, M.A., Rashid, A. (2019) Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers. *Software - Practice and Experience*. **50**(3), 275–298.

Yu, Y., Kaiya, H., Yoshioka, N., Hu, Z., Washizaki, H., Xiong, Y., Hosseinian-Far, A. (2018) Goal Modelling for Security Problem Matching and Pattern Enforcement. *International Journal of Secure Software Engineering*. **8**(3), 42–57.