LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

CC7178NI Cyber Security Management

Implementing Incident Response Management for Banking Sector

50% Coursework

Spring 2021

Student Name: Pravash Karki

London Met ID: 11071480

College ID: NP01MS7S210070

Assignment Due Date: 07th May 2021

Assignment Submission Date: 21st May 2021

Word Count (Where Required): 3500

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Abstract

The concept of incident response management is the first line of defence for any organisation against any unwanted incidents. In the modern world, where cyber-attacks and breaches are increasing daily, it has become essential for a financial organisation to prepare in advance to keep their data safe. At the same time, it is a well-agreed fact that incident response management is necessary for all kinds of organisation. There is still a debate about choosing a framework for incident response management for financial organisations. Due to the fact, there are multiple organisations with multiple frameworks and standards for incident response management. Therefore, this report defines the commonly used standards for incident response management and the best method to implement these standards. Also, this report illustrates the common problem that arises while implementing an incident response management framework for financial organisation. It also defines the effect, concerns, and solutions to these problems based on multiple reports, case studies, journals, and articles from experts.

Table of Contents

List of figures

List of abbreviation

CGAP	Consultative Group to Assist the Poor
CIS	Centre for Internet Security
CISO	Chief Information Security Officer
CSO	Chief Security Officer
ENISA	European Network and Information Security Agency
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
ISACA	Information Systems Audit and Control Association
NIST	National Institute of Standards and Technology
SANS	SysAdmin, Audit, Network, and Security
SOAR	Security Orchestration, Automation, and Response

1. Introduction:

1.1. Introduction to Incident Response Management:

Incident response management is the process of protecting the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems (CIS, 2021). In the current cybersecurity scenario, the ability to defend and handle cybersecurity incidents is taken as a measure to define how secure an organisation's data is. Hence, for this reason, incident response management plays a vital role in determining how secure an organisation is from external threats as it defines the level of readiness of an organisation to handle threats. Incident response management can be generally divided into several phases. These phases include the following:

- Preparation phase: This phase emphasizes preparing a solid plan to handle the incident and preventing incidents from happening by ensuring that systems, networks, and applications are sufficiently secure.
- Detection and analysis phase: This phase consists of step-by-step instruction to detect an incident and at the same time analyse the incident to prepare countermeasures.
- Containment, Eradication and Recovery: This phase focuses on containing the detected incident and eradicating it. This phase gives primary focus on recovering from the incident.
- Post-incident activity: This phase includes the significant activities that are to be performed once the incident is handled and the organisation recovers from the incident (Girken, 2019).

The following figure shows the different phases of incident response management:

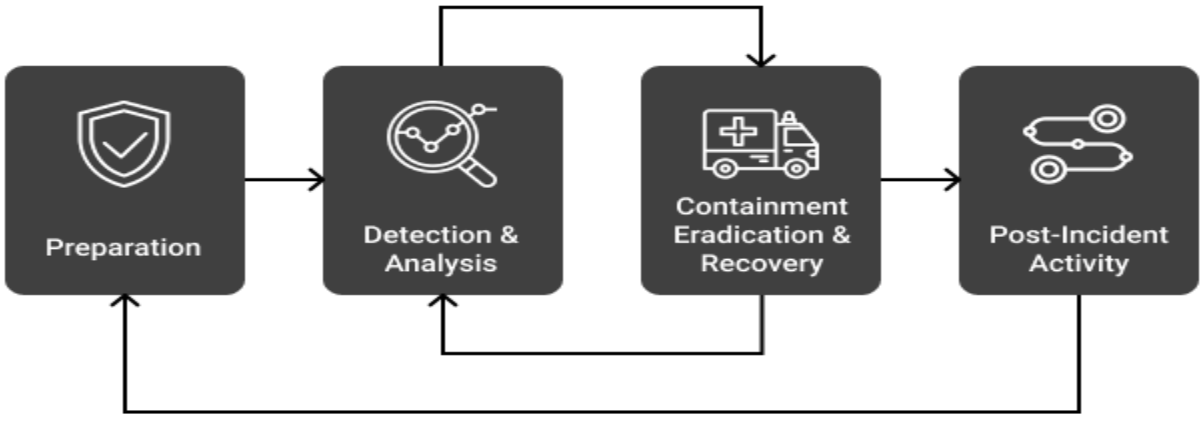

Figure 1: Incident Response Phase (UnderDefense, 2020)

1.2. Problems in Implementing Incident Response Management:

Incident response management is one of the most effective ways of handling incidents and making organisations cope with day-to-day cybersecurity attacks. However, implementing it in an organisation is one of the most challenging tasks. There are many organisations that have defined frameworks for incident response management. Some of the famous organisation that has given a framework for incident response and management include NIST, SANS and ISO/IEC and all of these frameworks have their positive and negative aspects (Geer & Sullivan, 2021). The NIST framework for incident response management divides the phases of incident response into four phases. The SANS, on the other hand, has divided incident response management phases into six (Girken, 2021). At the same time, ISO/IEC more or less defines the general practices and standards that need to be followed, unlike the NIST and SANS, which provides step by step guide to correctly implement the incident response management principle (Geer & Sullivan, 2021). So, the major problem when it comes to implementing incident response and management is finding the best practice and framework for incident response management.

1.3. Current scenario for implementing incident response management in financial sector:

In the same context, when it comes to implementing incident response management in financial sector, the major problem is different technology being used in each financial organisation. Every organisation in the world have their own security architecture which generally varies from other organisation due to various reason (Nikols, 2021). At the same time, the difference in the architecture does provide an organisation with safety from attacks. It also creates a hassle for implementing the incident response management frameworks and principles as there is a need to modify the framework for each organisation. This results in the cost of implementing the incident response management framework being high, which causes the organisations to hesitate in implementing incident response management. Especially in underdeveloped countries, high cost is the major reason for an organisation to refrain from implementing any new framework (MacFarlane, 2018). Therefore, it is crucial to either find a universally applicable framework or find incident response management principle which can be modified as per organisational requirement.

2. Literature Review:

The concept of finding the best practice and framework to implement in the banking sector is not a new one. There is commonly used incident response and management frameworks such as SANS and NIST. The NIST incident response management framework divides the overall incident response and management activities into four phases, while the SANS incident response management is divided into six stages. The NIST framework is commonly used by an organisation which are at the initial phases of implementing an incident response management framework. Similarly, the SANS incident response management framework is used by an organisation which are quite adept in using incident response management framework.

There have been quite a few researches done for finding the best way to implement incident response management in banking and financial institution. At the same time, multiple research papers can be found online. One of these research papers is titled 'Cybersecurity incident response capabilities in the Ecuadorian financial sector' published by Carnegie Mellon University, USA. This research paper defines the major problems that are prevalent in the Ecuadorian financial sector. This research paper also illustrates how to better cope with these problems to solve problems in implementing incident response management practices and frameworks.

Another similar research paper published by Twenty-fifth Americas Conference on Information Systems done in Cancun in 2019 titled 'Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis Completed Research Paper' defines the possibilities and issues in implementing incident response management in particular Ethiopian bank. Another whitepaper published by the UK finance represents the need of about 250 firms across the UK named 'Incident Management Cyber Incident Response - Is your firm ready', which defines the requirements for successfully implementing incident response management among various financial institutions across the UK.

Similarly, a research paper titled 'Financial Industry Examples Incident Response Team Activities in Finance' defines how the Japanese Company implements the incident response management practices in response to growing cybersecurity threats. Similarly, there is also a research paper published by SANS institute titled 'Incident Response Planning for Smaller Financial Institutions', which defines how to implement incident response management practices and standards effectively. There also guides represented by expert communities which define the proper way to implement incident response management practices.

However, all of these researches are focused only on solving implementation issues of a particular organisation. No research paper defines standard practices that any kind of financial organisation can use. And none of the available frameworks explains the problem that arises

while implementing them. Also, based on the research paper by CGAP with the title 'CYBERSECURITY IN FINANCIAL SECTOR DEVELOPMENT', it is clear that all types of organisations require an incident response management framework to cope with cybersecurity incidents. We can be clear that there is a need for a framework and practices for incident response management that any financial organisation can implement.

3. Critical Analysis:

According to the information provides by the CSO for the year 2020, sixty-three per cent of the companies said that their data was potentially compromised within the last twelve months due to hardware- or silicon-level security breach (Fruhlinger, 2020). This shows that attacks in the world have been increasing drastically. Therefore, financial companies, especially banks, must

adapt incident response management policy as it is the best solution when it comes to handling and management. However, to implement incident response management effectively, certain problems must be taken into consideration. These problems include:

3.1. Meeting the compliances:

To effectively implement incident response management principles and techniques, it is necessary to meet certain standards and requirements. For NIST, the requirement that must be met include access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, system and information integrity (Ross & Pillitteri & Dempsey & Riddle & Guissanie, 2020). Similarly, the SANS requires companies to follow CIS controls which is a prioritised, focused set of actions to help them stop most dangerous cyber-attacks and ensure data security (Grimes, 2019). Similarly, others standards of incident response such as ISO, ISACA, and so on also have their requirement. Yet, often it is seen that companies implement incident response frameworks without meeting the compliances. This results in a problem in the ineffective implementation of any applied framework and results in many loopholes in the security of the organisation, which will be used by the breacher. Ultimately, this ends up causing incidents that the organisation intended to mitigate (Davis, 2021). So, one of the major problems when it comes to implementing incident response management standards is the lack of compliance meeting.

3.2. Lack of Skilled Cybersecurity Professionals:

Throughout the world, the required manpower for the companies is in quite a shortage. According to a survey by CISO, including respondents of countries such as the US, the UK, Germany, Spain, Italy, Sweden, Finland, France, the Netherlands, Poland, Belgium, and the Czech Republic, there is a shortage in cybersecurity manpower. Thirty-three per cent of the respondent even said that they were hiring new talents, and forty-nine per cent expressed concerns that the shortage could expose their organisations to greater risks (TrendMicro, 2019). This fact shows that IT-related manpower is in shortage throughout the world. And, to further find an expert who is versed in multiple fields of IT, which is the requirement for incident management experts, is even more of a hassle. Furthermore, according to the research paper published by the International Labour Organisation titled ‘Skills shortages and labour migration in the field of information and communication technology in India, Indonesia and Thailand’, the needed ICT manpower for the developing countries is even more shortage (International Labor Association, 2019). This goes to shows that the required manpower for incident response management is quite less throughout the world. Hence, the financial institution such as banks and finances are not able to properly implement incident response management standards as the qualified person

to do so is missing. So, another problem for the successful implementation of incident response management is the lack of skilled manpower.

3.3. Lack of budget:

Another one of the major problems for incident response management throughout the world is the lack of budget for incident response management. It is a fact that incident response is one of the most critical factors for managing the security of an organisation, but still, it can be seen that organisation do not allocate the necessary budget for it. According to the IAPP-EY Annual Privacy Governance Report 2018, the average privacy budget had dropped from $2.1 million in 2017 to $1 million in 2018. Some of the common reasons for this massive decline include spending a large sum of money on the regulatory compliance preparation cycle or spending over the limit in the previous year (EC-Council, 2020). While this problem may not seem to have much impact on the incident response activities but poor incident response management can cost a lot. The negligence of having poor incident response management can cost an organisation a huge data breach which will cost the organisations hundreds of millions. The hesitation of spending a few million is very likely to have a huge impact on the data of the organisation (Paye, 2020). Therefore, the organisation must have a proper budget to spend on incident response management.

3.4. Lack of Proper risk management:

The proper implementation of risk management policies is the backbone of any organisation. The risk management policies define what the major threats that can occur in an organisation are and how to deal with them. In fact, in the preparation phase, which is the initial phase of incident response management, it is clearly stated that risk management of both hardware and software-related assets is mandatory (Girken, 2019). However, most organisation do no implement risk management strategies. And, there are issues even in the organisations that have implemented these risk management policies (Keqa, 2016). So, the prevalent problem for successfully implementing incident response management is the lack of proper risk management policy.

3.5. Lack of communication and collaboration between staff:

The process of incident response management requires a very good flow of information among the various department. When an incident occurs, the probability of it being found out totally depends upon the communication of departments. Some of the most effective processes by which incident are detected include studying daily reports from multiple departments, monitoring unusual activities among various department and analysing unusual activities reports from departments (Padayachee & Worku, 2020). So, when there is an absence of communication and collaboration among employees, there are chances of information flow among departments being delayed. Similarly, reports of suspicious activities based on monitoring can also be delayed

due to a lack of communication. This results in incident detection and response being delayed which can cause serious damages to the financial organisation as even momentary disturbance in day-to-day activities of the financial organisation can cause huge loss. Therefore, another one of the problems for effective implementation of incident response management is lack of communication and collaboration between staffs.

3.6. Lack of integrated monitoring tools:

The use of monitoring tools activities enables an organisation to monitor networks, servers, users and so on. It can be used to detect, identify and report various activities which may cause an incident. Furthermore, using an event-triggered monitoring system to alert for unusual activities is one of the measures for detecting incidents (Klein, 2019). However, often financial organisations do not integrate automated monitoring tools into their day-to-day activities. This is due to the fact that often employees consider monitoring tools invasive as it keeps track of records of every task of the employee (Dreyfuss, 2020). Another reason why organisations hesitate to integrate monitoring tools into their day-to-day task is cost. The cost of implementing monitoring tools in the past wasn't cheap, and due to this, the most organisation still have the stigma that implementing automated monitoring tools can be expensive (Solarwinds, 2021). Hence, despite the need for integrating monitoring tools for incident response management because of reason such as misunderstood cost and employee hesitation, lack of integrated monitoring tools is another problem for the implementation of incident response management.

4. Recommendations:

We can see that there are some problems when it comes to implementing incident response management standards and principles. However, if proper guidelines and recommendations are followed, then these problems can be solved. For the above-mentioned problem, the following are its solution:

4.1. Implementing standards which are verifiable:

While there many companies who all state that their incident response framework is best and most implementable. The problem is how to ensure their trustworthiness. According to a case study article titled 'An Operational Framework for Incident Handling' published based on the proceedings of the First Italian Conference on Cybersecurity (ITASEC17) held in Venice, Italy, the best method to measure the trustworthiness of any incident response management framework is based on their certification (Bottazzi & Italiano & Rutigliano, 2017). The article defines that using the framework which has a reliable and proven certification is the best method to ensure that an appropriate framework and standards that meet all compliance are implemented. Hence, the first things that any financial organisation must do are find a certified incident response management framework which fits their company's requirement. While there are many verified frameworks available, some of the most commonly used frameworks which are verified and certified are NIST, SANS and ISO/IEC.

4.2. Training available manpower:

The common idea that all companies and power have when it comes to choosing manpower for incident response management is hiring new manpower. But, throughout the world, there is a huge shortage of manpower (DFlabs, 2019). Hence, in such a scenario, the most effective method is to choose an incident response team from the available manpower. For this purpose, what can be done is to automate the everyday monitoring task and free up manpower and use that manpower for incident handling and incident management (ENISA, 2020).

4.3. Making an appropriate budget plan:

Another one of the most common problems, which is the lack of budget, can be solved by having appropriate plans and communication with the staff and workforce. Often, there is a hesitance in the upper management team to communicate with the staff. This leads to a poor plan being made for incident management for estimating the cost of incident response. This ultimately led to problems such as a lack of budget for incident response management, which can have disastrous consequences. Similarly, often neglect the activity of risk assessment which necessary for having a good budget plan for incident response management (Rose, 2020). Hence, another

activity the organisation must do to ensure proper implementation of incident response management is the improvement of communication of employees and team members along with proper risk assessment activities.

4.4. Ensuring risk management is done in every step:

One of the factors used to measure the effectiveness of incident response management and plan is risk management. Better risk management means the company or the organisation has better chances of handling incidents (UpGuard, 2020). Almost every certified and reliable framework for incident response management has mentioned that risk management is mandatory when it comes to the implementation of incident response management guidelines and framework. So, a financial organisation must ensure that proper risk management and assessment are done while planning for incident handling. This will ensure that incident response management implementation is done properly and without any errors.

4.5. Awareness and collaboration program:

The unwillingness of employee to communicate and collaborate with each other is often due to a lack of communication. An organisation usually do not conduct programs and training which enables employees of the different department to communicate and work with each other. Also, often superiors of respective department considering themselves superior because of lack of understanding of another department work. This leads to employees misunderstanding each other and ultimately leads to an unwillingness to corporate with each other. All these can be simply resolved if proper awareness and collaboration program is conducted on a regular basis (Bucata & Rizescu, 2017). Hence, the financial institution must conduct awareness and collaboration program on a regular basis to ensure that there are no while implementing incident response management practices and principles.

4.6. Using cost effective monitoring tools that protect privacy:

The misconception that the expensive history of automated monitoring tools is one of the major reason organisations hesitates to use automated monitoring tools (Solarwinds, 2021). However, various economic monitoring tools use various cost optimization strategies to provide cost-effective and efficient automated monitoring tools (Durand, 2020). The modern automated monitoring tools also provide a feature to only monitor certain aspects of employees, enabling employees to retain their privacy. Various laws throughout the world ensure monitoring tools will only monitor information related to the organisation and nothing else (Freedman, 2020). Hence, using these particular tools will help encourage an organisation to use automated monitoring tools and help in the effective implementation of incident response management standards.

4.7. Using automated defence mechanism:

It is physically impossible for a human to keep track of hundreds of alerts that come daily in an organisation. While most of these alerts may not be of high priority, there are some alerts which are crucial for organisation and failure address these alerts may cause huge loss to an organisation (Siemplify, 2018). Hence using an automated tool is the best solution to keep track of these alerts. Using tools such as SOAR (Security Orchestration, Automation, and Response), which provide automated alerts and respond to the incident, are the best method for an organisation to ensure that no unwanted incident occurs (Logsign, 2020). Similarly, a research paper published by the Technical University of Sofia, Bulgaria, defines that using Artificial Intelligence for automating incident response management will drastically improve the ability of an organisation to address and handle incidents. At same time using automated simulation for predicting incident is also very effective for improving incident detection (Trifonov & Yoshinov & Manolov & Tsochev & Pavlova). Therefore, an automated defence tool is another crucial factor that helps organisation properly implement incident response mechanism.

5. Conclusion

It is simply clear that while there are quite a lot of problems when it comes to implementing incident response management in the financial sector. These problems may cause organisations and financial institutions to hesitate from implementing incident response management practices and standards. But the benefit that implementing incident response management brings simply outweighs the minor problems that it may bring. If an organisation doesn't implement incident response management practices, then in times when it suffers from attacks and breaches, it will have no defence mechanism. This may cause the organisation to lose its overall data and may cause the organisation to go bankrupt. Hence, the company must implement incident response management practices.

Similarly, from the overall observation of the fact and figures, it was also made clear that that there is no single particular framework or standard for incident response management that can be implemented throughout the world. Since the diverse world has different kinds of problems, recommending one specific framework is not possible. However, it can be stated that if any financial institution may it be banks or finances or any other organisation, is at the initial steps of implementing incident response management, the best framework for them is NIST. Similarly, if the financial institution is well-versed in implementing the incident response management framework, it can implement the SANS framework. There is also the method of mixing multiple frameworks such as SANS, NIST, ISO/IEC, etc. This method is the best practice and provides the best result possible. But this process requires a lot of expertise and budgets to separate for incident response management. So, in a nutshell, it can be said that a financial institution such as a bank must first determine its budget and requirement. Then, it must estimate its needs, and based on that estimation. It can decide whether it is adequate to implement SAN or NIST or some other incident response and management framework.

6. References

Baur-Yazbeck, S., Frickenstein, J. and Medine, D. (2019). CYBERSECURITY IN FINANCIAL SECTOR DEVELOPMENT Challenges and potential solutions for financial inclusion. [online]. Available at: http://documents1.worldbank.org/curated/en/209721593689624542/pdf/Cyber-Security-in-Financial-Sector-Development-Challenges-and-Potential-Solutions-for-Financial-Inclusion.pdf [Accessed: 28th April, 2021].

BUCATA, G., RIZESCU, A. (2017). (PDF) The Role of Communication in Enhancing Work Effectiveness of an Organization. [online] Available at: https://www.researchgate.net/publication/316360042_The_Role_of_Communication_in_Enhancing_Work_Effectiveness_of_an_Organization. [Accessed: 12th May, 2021]

Bottazzi, G., Italiano, G. and Rutigliano, G. (2017). An Operational Framework for Incident Handling. [online]. Available at: http://ceur-ws.org/Vol-1816/paper-13.pdf [Accessed: 04th May, 2021].

Catota, F., Morgan, M., Sicker, D. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. [online]. Available at: https://www.researchgate.net/publication/324854058_Cybersecurity_incident_response_capabilities_in_the_Ecuadorian_financial_sector [Accessed: 24th April, 2021].

CIS. (2021). CIS Control 19: Incident Response and Management. [online] Available at: https://www.cisecurity.org/controls/incident-response-and-management/ [Accessed: 24th April, 2021].

Cynet. (2020). Incident Response SANS: The 6 Steps in Depth. [online] Available at: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/ [Accessed: 1st May, 2021].

Davis, A. (2018). Security vs Compliance: What's the Difference? [online] Available at: https://www.tripwire.com/state-of-security/security-data-protection/security-compliance-difference/ [Accessed: 2nd May, 2021].

DFLabs. (2019). Top 5 Incident Response Challenges SOAR Helps to Solve. [online] Available at: https://www.dflabs.com/resources/blog/top-5-incident-response-challenges-soar-helps-to-solve/ [Accessed: 4th May, 2021].

Dreyfuss, J. (2020). Here's how employers are using tech tools to keep a close watch on their remote workers. [online] CNBC. Available at: https://www.cnbc.com/2020/06/24/new-tech-tools-employers-are-using-to-keep-watch-on-remote-workers.html [Accessed: 12th May 2021]

Durand, M. (2020). The Best IT Monitoring Solutions Are Cost-Efficiency Tools. [online] Available at: https://www.centreon.com/en/blog/the-best-it-monitoring-solutions-are-cost-efficiency-tools/ [Accessed 13th May 2021].

EC-Council. (2019). 5 Common challenges incident response teams face. [online] Available at: https://blog.eccouncil.org/5-common-challenges-incident-handling-and-response-teams-face/ [Accessed: 3rd May, 2021].

ENISA. (2020). HOW TO SETUP UP CSIRT AND SOC GOOD PRACTICE GUIDE HOW TO SETUP UP CSIRT AND SOC. [online] Available at: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/at_download/fullReport [Accessed: 4th May, 2021].

Freedman, M. (2018). The Laws and Ethics of Workplace Privacy and Employee Monitoring. [online] Business News Daily. Available at: https://www.businessnewsdaily.com/6685-employee-monitoring-privacy.html [Accessed: 12th May 2021]

Fruhlinger, J. (2018). Top cybersecurity facts, figures and statistics for 2018. [online] CSO Online. Available at: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html [Accessed: 2nd May, 2021].

Geer, D., Sullivan, P. (2021). Building the best incident response framework for your enterprise. [online] Available at: https://searchsecurity.techtarget.com/tip/Incident-response-frameworks-for-enterprise-security-teams [Accessed: 26th April, 2021].

Girken, E. (2019). Incident Response Steps Comparison Guide for SANS and NIST. [online] Att.com. Available at: https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide [Accessed: 27th April, 2021].

GIAC. (2021). [online] Available at: https://www.giac.org/paper/gsec/3902/incident-response-planning-smaller-financial-institutions/106243 [Accessed: 27th April, 2021].

Grimes, R. (2019). The 5 CIS controls you should implement first. [online] CSO Online. Available at: https://www.csoonline.com/article/3438119/the-5-cis-controls-you-should-implement-first.html [Accessed: 1st May 2021].

International Labor Assoisation (2019). Skills shortages and labour migration in the field of information and communication technology in India, Indonesia and Thailand. [online]. Available at: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/publication/wcms_710031.pdf [Accessed: 26th April, 2021].

Krasnow, M. (2015). Guidance for Incident Response Plans | Expert Commentary | IRMI.com. [online] Available at: https://www.irmi.com/articles/expert-commentary/guidance-for-incident-response-plans [Accessed: 4th May 2021].

Keqa, A. (2019). 12 Reasons for Risk Management Failure. [online] Pecb.com. Available at: https://pecb.com/article/12-reasons-for-risk-management-failure [Accessed: 3rd May, 2021].

Klein, E. (2019). Monitoring and incident management: a winning combination. [online] Available at: https://logz.io/blog/monitoring-and-incident-management/ [Accessed: 13th May 2021].

Logsign. (2020). Automated Incident Response with SOAR - Logsign. [online] Available at: https://www.logsign.com/blog/automated-incident-response-with-soar/ [Accessed: 13th May 2021].

MacFarlane, D. (2018). The 3 hidden costs of incident response. [online] CSO Online. Available at: https://www.csoonline.com/article/3270940/the-3-hidden-costs-of-incident-response.html [Accessed: 29th April, 2021].

Mccarthy, J., Alexander, O., Edwards, S., Faatz, D., Peloquin, C., Symington, S., Thibault, A., Wiltberger, J. and Viani, K. (2019). Situational Awareness For Electric Utilities Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C). [online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-7.pdf [Accessed: 25th April, 2021].

Miyazaki, M., Hatanaka, H.,Takahashi, K., Nagata, M. (2016). Financial Industry Example Incident Response Team Activities in Finance. [online]. Available at:

https://www.hitachi.com/rev/archive/2016/r2016_08/pdf/r2016_08_105.pdf [Accessed: 26th April, 2021].

Nikols, N. (2021). Why your approach to security architecture needs to change. [online] TechBeacon. Available at: https://techbeacon.com/security/why-your-approach-security-architecture-needs-change [Accessed: 29th April 2021].

Padayachee, K. and Worku, E. (2020). Article 1 Information Security Incident Management: An Empirical Study on Ethiopian Organizations. The African Journal of Information Systems The African Journal of Information Systems, [online] 12(2). Available at: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1742&context=ajis [Accessed: 12th May 2021].

Paye, M. (2020). Poor incident detection can cost your organisation a fortune. [online] Available at: https://www.securitymagazine.com/articles/93173-poor-incident-detection-can-cost-your-organisation-a-fortune [Accessed: 3rd May, 2021].

Rose, J. (2020). How to Build a Case for Effective Cybersecurity Budgets. [online] Available at: https://www.tripwire.com/state-of-security/featured/building-effective-cybersecurity-budgets/ [Accessed: 4th May, 2021].

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. and Guissanie, G. (2020). Protecting controlled unclassified information in nonfederal systems and organisations. [online]. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf [Accessed: 1st May, 2021].

Solarwinds. (2021). The Expensive History of APM. [online] Available at: https://www.pingdom.com/blog/the-expensive-history-of-apm/ [Accessed: 12th May 2021].

Siemplify. (2018). Automated Incident Response - How Enterprises Benefit from it? [online] Available at: https://www.siemplify.co/blog/how-enterprises-benefit-from-automated-incident-response/ [Accessed: 12th May 2021].

TrendMicro (2019). Cybersecurity Skills Shortage a Problem for Nearly 50 Percent of Organisations - Security News. [online] Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-

threats/cybersecurity-skills-shortage-a-problem-for-nearly-50-percent-of-organisations [Accessed: 2nd May, 2021].

Trifonov, R., Yoshinov, R., Manolov, S., Tsochev, G., Pavlova, G. (2019). Artificial Intelligence methods suitable for Incident Handling Automation. [online]. Available at: https://www.researchgate.net/publication/335995496_Artificial_Intelligence_methods_suitable_for_Incident_Handling_Automation [Accessed: 12th May, 2021].

UK Finance. (2020). Incident Management INCIDENT MANAGEMENT Cyber Incident Response - Is Your Firm Ready? (2020). [online]. Available at: https://www.ukfinance.org.uk/system/files/Incident-Management-Whitepaper_FINAL.pdf [Accessed: 24th April, 2021].

UnderDefense. (2020). Incident Response Life Cycle [online] Available at: https://underdefense.com/incident-response-life-cycle-underdefense/ [Accessed: 26th April, 2021].

UpGuard (2019). What is an Incident Response Plan? [online] Upguard.com. Available at: https://www.upguard.com/blog/incident-response-plan [Accessed: 4th May 2021].

Yohannes, T., Lessa, L., Negash, L. (2019). Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis. [online] Available at: https://www.researchgate.net/publication/336133279_Information_Security_Incident_Response_Management_in_an_Ethiopian_Bank_A_Gap_Analysis_Completed_Research_Paper [Accessed: 24th April, 2021].