JOURNAL OF ITI CENTRE OF INTERNET TECHNOLOGIES (ICIT PNG)

Published by

INTERNATIONAL TRAINING INSTITUTE

Visit: www.iti.ac.pg

ISSN Number: 2707-9988

Editorial Board of ITI Centre of Internet Technologies (ICIT PNG)

Volume 1, March-April 2020
International Training Institute
Port Moresby
Papua New Guinea

Table of Content

S.No	Title/Author	Page No
1	***Assessing Cyber Security Risk in Digital Organization*** Kasiware Adam, Idam Brendon, Raku Dairus & Worinamiah Stanis	1-8
2	***A Study on Cyber-Attack and Information Protection in SMEs*** William M, Jack P, Emmanuel K, Joshua P & Ronald Y	9-12
3	***A growing concern for SMEs in Papua New Guinea- ICT Dilemma Context*** Joylyne.W, Bernice.B, Romana.U, Phillip.D & John Bosco.M	13-16
4	***Digital Security Technologies for Business Organizations in Papua New Guinea*** Elijah Ovasuru, Mika Inkharm, Michael Kereng, Gregory Passingan & Gedisa Kungkene	17-21
5	***A Survey on Managing Cyber Security Threats, Vulnerabilities and Risks within the Royal Papua New Guinea Constabulary*** Christoper Korgul, Cedric Robert, Crystal Matua, Manoji Maria & Augustine Porti	22-26
6	***Risk, Threats and Vulnerability of Cyber-Crimes in SME in Papua New Guinea*** Brown Maiwax, Mary Agua, Yuriel Bomai & Shaney Toinevane	27-31

Volume 1, No.1, March-April 2020 **ISSN:** 2707-9988

Journal of ITI Centre of Internet Technologies

Assessing Cybersecurity Risk in Digital Organization

Kasiware Adam[1], Idam Brendon[2], Raku Dairus[3], Worinamiah Stanis[4]
[1-4]Students, Diploma in Information and Communication Technology,
School of Information and Communication Technology, International Training Institute,
Papua New Guinea, enquires@iti.ac.pg

Abstract

Cyber Security is one of the most important practices that has been carrying out, in this modern technological world. However, in terms of Information and communication Technology, each and every organization should have a cyber-security to protect the organization's confidentiality information. Cyber Security helps the organization for functioning well and be manageable effectively in all the aspect of the business in terms of security. With that, in this study, we are going to discuss the Asset, Vulnerabilities, Threats, Risk, and implementation of appropriate information security mechanisms**.**

Keywords: Asset, Vulnerabilities, Threat, Risk, Physical Security Measures, Implementation

1. Introduction

Nowadays Information and Communication Technology (ICT) has become the most effective platform of communication with the internet as the medium with the support of the fastest growing technology which changes the face of the human environment. The advancement in technology has supported the occurring changes but most individuals and organizations are ICT illiterate that we can't safeguard our private information in an effective manner and perhaps cybercrimes are increasing day-to-day.

The modern computing activities such as e-commerce, banking, and cloud computing need a high level of security. Considering that modern technology kept much of critical personal data security is essential. There is nothing as absolute or one hundred percent security, the user only take measures to the level of their qualification to at least reduce breaches of critical information and the infrastructure of an organization to enlighten its wellbeing in the present and future as well. In order for Small and Medium Enterprises (SMEs) to become one of the most successful and well-secured then they must have security measures in a place to protect themselves as individuals and organizations from cybercriminal.

2. Asset

Assets are the things that have value in an organization and it can be anything tangible or intangible like an officer, a car, computers, security, software, rules, and regulations, etc. As per the study, we have interviewed Pacific Palms Property and had identified the type of asset and security measures that are in place to safeguard the organization. The physical assets are; Server, Router, Software both system and application software. The asset of Pacific Palms Property is classified into five categories:

a) **Hardware**
- Desktops
- Laptops
- CUG phones(link to computer)
- Projectors
- Flat Screen for presentation in internal staff meetings
- Routers & Switch

b) Systems

- Pronto System(Finance) AP(Account payable), AR (Account receivable)
- HR Portal(Policy and procedures)

c) Service and Applications

- Microsoft office
- E-mails
- Visio used to do up organizations chart

d) Valuable Information

- Trade secret
- Employees data
- Meeting minutes

e) Others

- General manager
- Employees

3. Vulnerabilities

Vulnerability is any weakness of an asset in the organization which may be exposed to the possibility of being attacked or harm by intruders. Now that we have identified the organization's asset and inventoried the threat, we need to find out the vulnerability of your system. Every system has vulnerabilities. Identifying assets specific vulnerability is a major part of risk assessment. After assessing the threat and vulnerabilities of your assets the result will provide the information you needed to decide what security measures are appropriate for your organization. However, in terms of physical security, the organization is highly secured with security guards of ESS (Executive Security System) with CCTV cameras and CUG (Closed User Group) phones for alarming any danger to notify employees and biometric systems to gain access in and out. But only major vulnerability faced by the organization is the scam emails.

If the access control mechanism of the virtual machine fails, a hostile applet can be given access beyond the sandbox (as described in (McGraw and Felten 1997). In such a case, the operating system will allow the hostile applet full access to the user's file because of the operating system there is no difference between the virtual machine and the applet. In such cases, there will be a clear violation of expected cumulative access control rules. (Bishop and Bailey 1996) proposes a state-space definition of vulnerability.

4. Threats

Identifying threats is a key part of security risk assessment. The best strategy to assess the level of threat to your system is to evaluate the magnetic force that attracts possible intruders into your organization's standard security measures. The threat comes in different formats based on the nature of the attack.

They can be classified as;

1. Malware
2. Security breaches
3. Dos attacks
4. Web attacks
5. Session hijacking
6. Insider threats
7. DNS poisoning

After classifying the form of threats that will be harmful to the organization, make sure that you can be able to take some actions to battle the threat. If your organization is capable and ready to face then go ahead and implement your organization's safety measures.

In a certain time, a computer virus has been the most likely threat to individuals and organizations with the fact that every month emerging viruses are documented. The situation proves that emerging viruses are being invented but the old ones are still functioning out there. However, such a very common attack like spyware is becoming a vast problem even enormous than viruses. The biggest threat identified in the organization is an online scam which is supported by the unnecessary email pop-ups.

5. Risks

Risk is any vulnerability exposed to the threat. The organization that we have interviewed and identified that they are well secured with standard security measures and policies. But the major problem is the use of emails with unwanted emails or pop up ads that they cannot overcome. This means it has become a risk to the organization if they accept it unintentionally may now become a major threat to the organization. The organization has the four (4) ways to assess the risk, whether to;

- Avoid the risk
- Accept the risk
- Transfer the risk
- Reduce the risk

6. Physical Security Measures

Physical security measures are the security policies that are in place to safeguard the organizations' physical assets.

The Computer Service Division of Pacific Palms Property gives training to their staff and sending random emails to test them, if they happen to open it, they would face some consequences and policies in place to avoid viruses and other threats.

As identified in Pacific Palms Property their security measures are bio class for clock-in and clock-out, access card connected to the CUG phone to get a notification if something went wrong in the organization which is also attached with ESS (Executive Security System) for any external threat to the organization.

8. Security Policies

A security policy could be a document that defines how an organization will cope with some aspect of security. There are often policies regarding end-user behavior, IT response to incidents, or policies for specific issues and incidents based on cyber activities.

Security policies may also be created to cope with regulatory requirements. These varieties of policies direct members of the organization on the way to suits certain regulations. A good example; can simply be advisory, suggesting to employees how they should handle certain items, but not requiring compliance. For example, a policy might advise users that emailing from a smartphone using a Wi-Fi hotspot can be insecure, but not forbid able.

8. Defining User Policies

One major code to keep in mind is to evaluate user's policies in every possible situation.

Failure to have policies that address a given problem will usually result in that problem being exacerbated. Something may seem like common sense to you but may not be to someone without any training or experience in computer networks or network security.

The misuse of systems is a major problem for many organizations. A large part of the problem comes from the difficulty in defining exactly what misuse is. Some things might be obvious misuse, such as using company time and computers to search for another job or to view illicit websites. However, other areas are not so clear, such as an employee using his/her lunchtime to look up information about a car he/she is thinking of buying. Effective usage policies should usually explain clearly how people can use the program and how they should not. It needs to be very straightforward and fairly precise for a policy to be successful. Vague claims such as 'computers and access to the Internet is for business use only' are clearly insufficient. We would recommend something more clear and perhaps more enforceable, perhaps something like “computers and Internet access is only for business purposes during business hours. However, during the non-working hours, workers can use the computer / Internet connection for personal use, such as breaks, lunch, and before work. Such usage must, however, be in compliance with policies on Internet usage. "That is transparent, direct, and enforceable.

Other areas for potential misuse are also covered by user policies, including password sharing, copying data, and leaving accounts logged on while employees go to lunch, and so on. All of these issues ultimately have a significant impact on your network’s security and must be clearly spelled out in the organization’s user policies. Stated below are of the identified several areas that effective user policies must cover:

■ Passwords

■ Internet use

■ Email usage

■ Installing/uninstalling software

■ Instant messaging

■ Desktop configuration

■ Bring Your Own Device

8.1 Defining System Administration Policies

In addition to deciding user policies, network administrators ought to have certain clearly defined policies. There has to be a method to attach users, delete users, address security problems, and alter some programs, and so on. Standards must also be in effect for treating any deviations.

8.2 New Employees

When a new employee is hired, clear measures to safeguard company security must be established in the system administration policy. New workers must be provided access to the tools and applications needed by their job roles. You need to record the granting of that access (possibly in a log). It is also important that the new employee receives a copy of the Software Security / Acceptable Use Policy from the company and signs a document acknowledging receipt.

Before a new employee starts to work, the IT department (specifically network administration) should receive a written request from the business unit that the person will be working for. That request should specify exactly what resources this user will need when he/she will start and have the signature of someone in the business unit with the authority to approve such a request. Then the person who is managing network administration or network security should approve and sign the request. After you have implemented the new user on the system with the appropriate rights, you can file a copy of the request.

8.3 End of Contract

When an employee leaves, it is critical to make sure all of his/her logins are terminated and all access to all systems is discontinued immediately. Unfortunately, this is an area of security that all too many organizations do not give enough attention to. You cannot be certain which employees will bear the company’s ill will and which won’t upon leaving the company. It is imperative to have all of the former employee’s access shut down on their last day of work. This includes physical access to the building. If a former employee has keys and is disgruntled, nothing can stop him from returning to steal or vandalize computer equipment. When an employee leaves the company, it is necessary to ensure that the following actions take place on his/her last day at work:

Defining System Administration Policies

■ All logon accounts to any server, VPN, network, or other resources are disabled.

■ All keys to the facility are returned.

■ All accounts for email, Internet access, wireless Internet, cell phones, and so on are shut off.

■ Any accounts for mainframe resources are canceled.

■ The employee's workstation hard drive is searched.

The end item always seems odd. But fortunately, if an employee gathered propriety company's data with him/her or attempting to any illegal activity you need to discover it immediately. If it is evident you must indeed secure that workstation and preserve it for the proof of criminal activity which is taken by the employee. It is extreme but repays doing which is realistic with the vast number of employees without any considered issues. However, if you don't make it a mode of securing your employee access when departing eventually you will face the problem that you could solve easily.

9. Change Requests

The nature of information technology is change. Not only do end-users come and go, but expectations always change. Business units require access to various services, server administrators update software and equipment, new software is built by application developers, and web developers change the website. Change happens all the time. Hence it is important to have a process of change control. The method not only helps the transition run smoothly but also allows IT security staff to review the transition before it is introduced for any possible security issues.

▪ A request for change control will go through the following steps: The request is signed by an appropriate manager within the business unit, ensuring the request is accepted. In other words, there is no point in pursuing the change request process if the immediate supervisor of the requestor has not approved the request.

■ The appropriate IT unit (database administration, network admin, email admin, cloud administration) verifies that the request is one it can fulfill technologically, fits within budget constraints, and does not violate IT policies.

■ The IT protection unit is testing that this move does not cause security issues. In modern times, that is becoming more and more critical.

■ A strategy to enforce the change is devised by the correct IT team, and a strategy to roll back the change in the event of failure. The latter part is highly critical and is often overlooked. Any process must be in place to roll back the change should it cause any problems.

■ The date and time for the change are scheduled, and all relevant parties are notified.

Your change control process might not be identical to this one; you may actually be far more precise. The thing to note, however, is that in order for your network to be safe, you simply cannot allow changes occurring without some mechanism to analyze the effect of those changes before they are enforced.

Change management operations are sometimes handled by a mechanism called a Change Control Board (CCB), often called a Change Approval Board (CAB). The basic process of change can be summarized as follows:

■ Initiated with RFC document (Request for Comments or Request for Change)

■ RFC sent for approval

■ Priority is set

■ Assigned to whoever makes the change

■ Document decisions

■ Evaluate by CAB

■ RFC scheduled

■ Complete when change owner and requester verify the successful implementation

■ Review of RFC

10. Defining Access Control

Access control is an important field of the security policy that creates a bit of controversy in every organization. There is often a tension between the desire of users to have free access to any data or resources on the network, and the obligation of the security administrator to secure those data and resources. That means extremes are not realistic in policies. You cannot simply lock as absolutely as possible any resource because that will hinder the user's access to those resources. Conversely, you can't just give full access of anything to anyone and everyone. Each person is given the minimum privileges necessary to do his/her job. No more and no less.

This is where the least privileges concept comes into play. The idea is simple. Each user, including IT personnel, gets the least access he/she can have and still effectively do his/her job. Rather than ask the question, "why not give this person access to X?" you should ask, "Why to give this person access to X?" And if you don't have a very good reason, then don't. This is one of the fundamentals of computer security. The more people that have access to any resource, the more likely some breach of security is to occur.

Along with, and related to, least privileges are the concept of implicit deny. Implicit deny means that access to network services is implicitly denied to all users unless expressly granted by an administrator.

Service separation, work rotation, and compulsory holidays are all relevant and related concepts. Duty separation means no one can carry out vital tasks; at least two people are required.

This prevents one person from accidentally, or intentionally, causing some security breach via inappropriate use of critical functions. Both job rotation and mandatory vacations are used to make sure that, periodically, the person performing a given job change. This makes it more difficult for one person to exploit his/ her position to breach security.

Obviously, trade-offs must be made between access and security. Examples abound. One common example involves sales contact information. Clearly, a company's marketing department needs access to this data. However, what happens if your competitors get all of your company's contact information? That could allow them to begin targeting your current client list. This requires a trade-off between security and access. In this case, you would probably give salespeople access only to the contacts that are within their territory. No one other than the sales manager should have complete access to all the marketing data.

11. Developmental Policies

IT (Information Technology) departments are made up of programmers and web developers who also develops most security policies had never address encrypted programming. It doesn't matter the integrity of your firewall, proxy server, virus scanner, and policies could be assuming if your programmers developed weak code you'll accord security breaches. However, we can contemplate a concise registry for elucidating shielded advancement regulation.

Assuming your company contemporarily has in secured development ambition the concise registry will definitely be enhanced rather than programming in a void.

Additionally, it can be a reference point to get you to discuss convenient programming:

■ All code, especially code done by outside parties (contractors, consultants, and so on) must be checked for backdoors/Trojan horses.

■ All buffers must have error handling that prevents buffer overruns.

■ All communication such as using Transmission Control Protocol (TCP) sockets to send messages must adhere to your organization's securing communications guidelines.

■ Any code that opens any port or performs any sort of communication is thoroughly documented and the IT security unit is apprised of the code, what it will do, and how it will be used.

■ All input is filtered for items that might facilitate an attack, such as a Structured Query Language (SQL) injection attack.

■ All vendors should supply you with a signed document verifying that there are no security flaws in their code.

Following these guidelines will not guarantee that flawed code is immune from being introduced into your system, but it will certainly lower the odds significantly.

12. Conclusion

To conclude, network security is a complex and constantly evolving field. Practitioners need to remain on top of new threats and approaches and be vigilant in risk assessment and network security. The first step in understanding network security is getting to know the actual threats faced to a network. Without a realistic idea of what the threats could affect your systems, you will not be able to protect them effectively.

All subsequent security decisions are informed by the attitude you take towards security and set the tone for the network security architecture of the entire organization. Let us take a moment to examine a few concepts that should permeate your entire thinking about security.

The first concept is the CIA triangle. This does not apply to covert activities involving the Central Intelligence Agency; instead, it is a reference to the three security pillars: secrecy, honesty, and availability. When you think about security, these three principles should always direct your thinking processes. First and foremost, are you keeping the data confidential? Does your approach help guarantee the integrity of data? And does your approach still make the data readily available to authorized users?

A different concept to think of is a minimal advantage. Precisely all users or services that are active on your network must possess not all but the limited figures of advantage/access needed to perform his / her duty. None should be granted access to other documents but except it is totally needed for the job which is referred to as "Need to Know" in military and intelligence.

Abbreviations:

CAB: Change Approval Board
CCB: Change Control Board
CCTV: Closed Circuit Television
CIA: Confidentiality, Integrity & Availability
CUG: Closed User Group
ESS: Executive Security System
IT: Information Technology

RFC: Request for Comments or Request for Change
SQL: Structured Query Language
TCP: Transmission Control Protocol
VPN: Virtual Private Network

References

1. Easttom, C. (2016). *Computer Security Fundamentals.* United States of America: Pearson Education, Inc.

2. G.Nikhita A Reddy, G. R. (2014). *A Study Of Cyber Security Challenges And Its Emergning Trends On Latest Technologies. Research Gate*, 201-203.

3. Krsul, I. V. (1998). *Software Vulnerability Ananlysis.* Purdue University.

4. Minnesota. (2018, December 2). *Study Blue.* Retrieved from Study Blue: https://www.studyblue.com/notes/note/n/chapter-10/deck/13066961**.**

5. Vaishnavi J.Deshpande, D. S. (2014). Cyber Security: Strategy to Security Challenges- A Review. *International Journal of Engineering and Innovative Technology (IJEIT)*, 290-292.

Volume 1, No.1, March-April 2020 **ISSN:** 2707-9988

Journal of ITI Centre of Internet Technologies

A Study on Cyber-Attack and Information Protection in SMEs

William M[1], Jack P[2], Emmanuel K[3], Joshua P[4], Ronald Y[5],

[1-5]Students, Diploma in Information and Communication Technology,
School of Information and Communication Technology, International Training Institute,
Papua New Guinea, enquires@iti.ac.pg

Abstract

Small and Medium Enterprises (SMEs) represent a large proportion of the Nation's business activities. There are many reports, reporting the threat to business from cyber security issues resulting in computer hacking by hackers that greatly achieved system penetration and information compromise. Even some are focused on surveying the actual SMEs themselves and attempts to improve SME outcomes with respect to cyber security. This paper represents research in cyber security attacks on SMEs, particularly Vulnerable to cyber-attack.

***Keywords**: Cyber Security, Vulnerabilities, Ransomware, Cyber Insurance*

1. Introduction

Cyber-attacks on small businesses may not receive the same level of media attention as attacks on large corporations, but small businesses are a prime target for hackers around the globe. It is estimated that 43 percent of all cyber-attacks involve small business victims. Most small enterprises still have no cyber security infrastructure in place to avoid or recover from attacks, making it a relatively easy exercise for attackers to penetrate private data ne tworks of small businesses and access anything including customer records, credit card information and intellectual property.

Cyber security threats are the way a scammer tries to steal money or data from the company or even from the clients. Performance for a scammer may be the downfall of a company. It is good for small business owners to implement necessary cyber security policies and practices. And they must also take time to educate themselves and their staff.

2. Cost Associated with Cyber Security and Cyber Attacks

For many businesses, expensive cyber security products are the first to go on the budgetary chopping block. But forgoing data security because of budgetary limitations can have severe consequences. Statistics indicate that 60 percent of small businesses who fall victim to a cyber-attack go out of business within six months, meaning that would-be hacker have everything to gain while small companies have to risk their clients, jobs and livelihoods.

Costs are one part of the dilemma small companies have to support themselves, and the other part is access to manpower. Small businesses frequently report that they struggle to find qualified cyber security professionals to keep their data well-protected. Around the globe, there are more than 300,000 unfilled cyber security jobs with demand rising each year.

A single data breach has a financial effect on small and medium-sized companies according to Kaspersky Labs. Hackers also want money, or access to accounts. Yet the data of the businesses is more important than that the company owner's information, as well as their customers or customers' personal identifiable details. In addition to net phishing, a hacker would likely want the credit card information of the customers.

3. Ransomware and Malware on SMEs

The system is the responsibility of each individual employee in a working organization (Robert M.Clark, 2017). Also, some of the SMEs adopt consumer products for safeguarding from the cybercrimes and that provide only basic protection.

What's most important to remember is that hackers do not always care about the data from a company. They only want their data and other sources because they know it's valuable to the business. So, the question is, how important the data is to the owner of the company, and what are they willing to pay to get back that data? This strategy is what called as ransomware a rising cyber-attack.

Though, ransomware is very common in all developed and developing countries. All cyber security breaches cause damage to business owners. The violation can cause financial harm or the credibility of the companies until the attack is made public. Malware can be sent via a link or attachment to an employee's email. Once a virus is released, it is downloaded into the business computer network, damaging data of the company in some way or giving access to the scammer.

Therefore, it's critical to train employees. This includes making business transactions a transparent event, where a manager or employee must check with others before making a significant transaction or releasing the information. Furthermore, businesses have to train employees annually on scams and how to manage the situation. And lastly, keep the communication lines open on this issue.

4. Vulnerabilities

Now, you may think, “I’m a family-run, small business, what does a hacker want with me?” I believe you’re not a priority. Con artists depend on knowledge gaps, misunderstanding and preparedness among small business owners and their employees to perpetrate scams with success. The research available on the topic suggests small businesses are particularly vulnerable to scams. A small business does not report scams, is likely to be subject to repeated attacks and is particularly susceptible to online fraud.

Some of the business reports are having cyber security measures in place, according to the BBB, 2017 State of Cyber security among Small Businesses report. These interventions included antivirus, firewall tools and training for the employees. In fact, BBB certified companies are almost three times more likely to have information security insurance coverage.

5. To protect your business, here are some of the steps to take

5.1 Train Your Employees

- Needless to say, your employees are the biggest source of vulnerability if you don’t train them in cyber security best practices.
- Just imagine the risk of your employee leaving work phone/laptop/tablet unattended in a public place. It can detrimentally harm your company.
- So you should educate your employees on cyber security.

Here are some tips:

- Clearly communicate the impact of a cyber-incident of your business
- Make cyber security everyone’s responsibility
- Have regular cyber security sessions in your office
- Train your employees on how to respond to a cyber-attack

5.2 Keep Your Software Up-to-date

Small businesses should always keep their software applications up-to-date because doing so is critical for cyber security.

Hackers and cybercriminals keep on looking for software vulnerabilities to take control of data, hack the important data, or encrypt your files to demand money.

Software updates patch the holes in security to keep hackers at bay. Not only can you upgrade the software applications installed in your office but also make sure your remote workers keep their software applications up-to-date.

And the next time you see a prompt to upgrade apps, never click on notify me later.

5.3 Secure Remote Access

Telecommuting is on the rise because the way we function has changed.

You may have staff employed remotely, as a small business owner. To those who access it remotely, you can ensure that data and system remain secure.

Without securing remote access, you cannot boost the cyber security for your business.

The followings are some remote access security measures you can implement to make remote access secure:

- Use a strong firewall and security software
- Review server logs to monitor remote access for any unusual activity
- Limit remote access to the minimum functions required
- Restrict remote access to unauthorized users
- Use at least two-tier authentication

Unless you don’t proactively protect it, remote access will expose your small business to a lot of cyber security risks.

5.4 Create Backup Files of Critical Business Data

Cyber-attacks could happen even though you follow best practices in cyber security. And, for sensitive business records, you can create backup files.

Regular backup of the sensitive data from all the computers are mandatory to be protected from threat. Records contains sensitive data in the form of word processing, electronic spreadsheets, databases, financial reports, human resources reports and receivable or payable account files. Organization should enable automatic backup in regular interval and to store the copies either offsite or in the cloud.

Here are some tips on data backup for small businesses:

- Store backup data on the cloud
- Check the backup regularly to ensure it is working properly
- Keep the backup encrypted and protected
- Make sure your data backup strategy is up-to-date

Small businesses facing a poor blow from cyber-attacks with a strong data backup plan as compared to those without data backup.

5.5 Purchase Cyber Insurance

It goes without saying that, to stay safe, you need to follow best practices in cyber security.

However, cybercriminals are keeping up with the new technologies and small business software applications to improve cyber security.

So it is imperative that you should buy cyber insurance to protect your business against losses resulting from a cyber-attack.

Typical first-party cyber insurance provides coverage for a data breach (like theft of personal or business information), cyber-attacks on your data held by vendors, cyber-attacks happening anywhere in the world that might affect your digital infrastructure, etc.

And finally the third-party coverage offers compensation to individuals affected by a data breach, expenses arising from a claim and settlement, cost of litigation, etc.

6. Conclusion

Small companies have more digital assets than individuals but less protections than big businesses have. Therefore, hackers find easy to target small business owners because there is a lack of security risk. Implementing security risks is a good practice in order for organizations to be safe from different types of attacks.

So, business enterprises should buy the latest antivirus and other cyber security tools to fight cyber-attacks. It is good idea to rule out any vulnerability by getting the digital infrastructure periodically reviewed by a cyber-security expert for any security loopholes.

Every small business needs cyber protection nowadays, as hackers are targeting small business increasingly.

Abbreviation:

BBB: Better Business Bureau

SMEs: Small and Medium Enterprises

References

1. F.Smallwood, R. (2009). *Safeguarding Critical E-Documnets: Implementing a Program for Securing.* United States.
2. Franklin D.Kramer, S. H. (2015). *Cyberpower and National Security.* Washington D.C.
3. Manson Benedict, R. E. (1971). *Science and Public Affairs.* China.
4. Ping, P. (2017). *World Internet Development Report.* China: Chinese Academy.
5. Robert M.Clark, S. H. (2017). *Cyber Physical Security.* Switzerland: Springer International Publishing.
6. S.Nevid, J. (2013). *Psycholog and Applications.* USA: Wadsworth, Cengage Learning.
7. https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html

Volume 1, No.1, March-April 2020 **ISSN:** 2707-9988

Journal of ITI Centre of Internet Technologies

A Growing Concern for SMEs in Papua New Guinea- ICT Dilemma Context

Joylyne.W[1], Bernice.B[2], Romana.U[3], Phillip.D[4], John Bosco.M[5]
[1-5]Students, Diploma in Information and Communication Technology,
School of Information and Communication Technology, International Training Institute,
Papua New Guinea, enquires@iti.ac.pg

Abstract

Cyber-attack is a major security risk for the business organization including SMEs. Research shows that Small and Medium Enterprises (SMEs) have become the main targets for cyber attackers and small businesses are prime victims that are left vulnerable to major security risks and threats.

Sometimes, the damage is done deliberately by misuse of data or unintentionally, for instance, an employee accidentally corrupts a valuable file. SMEs may also be unsuccessful due to service provider problems as well as database management issues.

In order for SMEs to minimize these attacks, certain standards can help to reduce the risks and threats as well as protect the business from suffering from cyber-related loss.

Keywords: *SME, ICT, ISP, Security, Network.*

1. Introduction

The term security is defined as ‘the condition of being threatened, especially physically, psychologically, emotionally or financially’. This article will give a crystal-clear on the problems and issues are faced by the SMEs and other business organizations. Our group has undergone the task of visiting the various SMEs to interview and identify the issues they face with the current IT security systems and policies. We are assigned the task of going to various small and medium-sized enterprises to interview and find out what type of issues they face with their current IT security systems and policies.

The aim of this article is to identify the main problem and outline it by stating the type of issues or threats the SMEs face on a daily basis. After going through certain organizations and SMEs, we have come up with some of the main issues that the organizations or SME’s are facing and how to address them.

This article outlines the issues and threats faced by the organizations.

2. Reason for Network Failure

Networking issues cannot be avoided within SMEs. Both organizations and SMEs deal with problems such as an employer cannot send an email or access the internet to do a transaction, which broadcasts an overview that networks are bound to face flounders and that it can be maintained and resolved quickly the next time around.

With regard to (Wanai, 2019), it was also mentioned that most of the network fails due to the usage of legacy systems (old computers and servers) in organizations. Networks can potentially grow and the need to update a network can be costly. This is the very reason why most SMEs and organizations still using outdated networks.

The growing trends in technology is a must that they upgrade their networks to avoid future setbacks and unnecessary costs.

3. Lack of Internet Service Providers (ISPs)

The interviewee also pointed out that there weren't enough internet service providers (ISPs). SME today faces a growing concern that there aren't many ISPs available.

According to (Wanai, 2019), although the current ISP's like Digicel, Be-mobile, Telikom PNG & Daltron provide internet services, SMEs still cannot afford such rates that are provided by these ISPs. This prompted them to stick with the local market and use social media as their platform to advertise their products and services.

According to another interview with Miss Mattlean (Mage, 2019); and Mandana (Sauwa, 2019), both SME owners who use the social media platform to advertise their products. They have stated further that the most common threats they face while marketing their products online is strategy ideas were stolen by other well established SMEs since they cannot settle the rates provided by certain ISPs, they have no choice but to use this platform without security.

Known organizations such as Bank South Pacific (BSP) advertise their plans and service structure through the ISPs to host their websites, to do internet banking and advertise their services as mentioned above to the public by giving them sufficient services like online transactions.

Providing more ISPs along with convenient rates can make way for SMEs to advertise their products and services to both the urban and rural areas.

4. Database Systems

Another issue identified by the organizations was that there wasn't any proper database system in place. Almost all organizations including SMEs need to keep track of their data records and maintain their transactions on a daily basis.

Without a proper database system, retaining data can be difficult to maintain. Both the employer and employee need their data to be kept safe, secure and confidential.

Bilas Fashion (Tamanabae, 2019), a national trending SME who also use the social media platform to market and advertise their products stated that they have no proper database system in place to keep records of client's bulk orders as well as employee and employer records due to the costs of employing a database manager.

A database ensures that all the data is kept and maintained in a central location so that both organizations and employees are on the same page regardless of time and place. SMEs need proper database management systems (DBMS) to assist them with their clients and to keep track of its performance.

5. Integrating Infrastructure

Information Technology infrastructure also provides a wide range of tools to help SMEs for their growing needs. Infrastructure is the only foundation that helps to build an organization or an SME to grow and classify the needs and wants of a particular firm.

Companies rely on technologies like broadband internet services to advertise and market their products to the public. The concern was that this need to be implemented to account for SMEs so that they could be also on the market domestically.

The interviews gave us an insight as to how IT infrastructure plays a huge role in most organizations and which led to greater company earnings. SMEs need infrastructures such as broadband internet services, fibre optics, VoIP, video conferencing and web services to boost them to a certain degree in order to maintain their competitive advantages.

6. ICT User Role

The information user role is quite the issue which identified to be a trend within organizations and

SMEs. Almost all employees within the firm have at least a minimum experience with the knowledge and skills needed in order to use technologies. To be an ICT skilled and literate, employers must be able to comprehend and understand the technologies they are using. At least 1 in 8 employees are said to be ICT illiterate and are mostly associated with employees who are well beyond the age of 47-55. Some employees cannot performance Simple tasks like sending an E-mail and downloading an image so that they have to be trained in order to keep the business operation running.

Furthermore, this can have a huge impact on the organizations or SMEs in which simple human errors could cause tremendous costs and even its reputation.

Addressing network technicalities and performance is usually done by IT professionals within the company. Providing the best IT skill to address an issue or fault in a firm's network can be done by its IT department. Such issues also identifies that the staff employed need to be IT certified in order to accomplish simple and tedious tasks when required.

Firms need to be conscious of the type of ICT individuals they hire or employ who proclaim to be IT certified but do not deliver ICT skills at a professional level. All IT staff must be adequate to address any fault in the network and be able to do repairs and diagnose any problem.

The IT staffs also need to be qualified and reviewed to be able to handle IT-related work such as network performance or any ICT work-related matters. Tasks such as checking cables, configuring a router or connecting PC's to the internet requires professional ICT skills.

This showed us that most organizations and SMEs (recruiting the IT professionals and outsourcing the software to develop and deliver) do hire other IT professionals to do what their own could not deliver (e.g. software outsourcing).

Various interviews gave us in-depth knowledge about how businesses and SMEs operate and the difficulties they face, thus issues related to IT and how they address them. The most interesting fact about these interviews are that our batch mates had the experience to discover ICT in a new perspective and its uses in organizations and SMEs.

7. Recommendation

We the group, strongly recommends that small and medium-sized enterprises need more awareness about the issues that both organizations and SMEs face.

With the proper tools and awareness, the business can identify the issues at first and able to overcome the setbacks.

It is vital to identify the early risks/issues to avoid unnecessary setbacks and lead to more productivity and as well as better performance as a whole.

8. Conclusion

To conclude, SMEs are facing a lot of issues because there is not enough infrastructure, services, and awareness to cater the growing demands of small enterprise businesses. This leads to a lot of setbacks and face a much harder competition to keep its clients or customers. With that being said, larger organizations have a much greater advantage over SMEs. But the SMEs can result in bankruptcy that lead towards business closeout because of cyber threat and attack.

Abbreviations:

ICT: Information and Communication Technology

ISP: Internet Service Providers

SME: Small and Medium Enterprises

VoIP: Voice over Internet Protocol

DBMS: Database Management System

BSP: Bank of South Pacific

References

1. Mage, M. (2019, September 21). *M's Handmades; Jewellery & Watches.* (B. Bawo, & P. W. Dobunaba, Interviewers)
2. Sauwa, M. (2019, September 13). *Manda's Hand Creations; Local Business.* (B. Bawo, Interviewer)
3. Tamanabae, B. (2019, September 25). *Bilas Fashion; Clothing Brand.* (B. Bawo, & R. Urum, Interviewers)
4. Wanai. (2019, October 15th). *National Broadcasting Corporation.* (J. Wanai, & J. B. Maur, Interviewers)
5. www.degruyter.com/downloadpdf/j/manment (December, 2017)
6. www.globalknowledge.com/us-en/resources/(2013, January)
7. www.skillspanorama.cedefop.europa.eu/en (December,2016)
8. www.allmoneymakingideas.com/problems-and-challenges-faced-byemployees-at-work/Career Change(August, 2019)

Volume 1, No.1, March-April 2020 **ISSN:** 2707-9988
Journal of ITI Centre of Internet Technologies

Digital Security Technologies for Business Organizations in Papua New Guinea

Elijah Ovasuru[1], Mika Inkharm[2], Michael Kereng[3], Gregory Passingan[4], Gedisa Kungkene[5]
[1-5]Students, Diploma in Information and Communication Technology,
School of Information and Communication Technology, International Training Institute,
Papua New Guinea, enquires@iti.ac.pg

Abstract

Business organizations becomes digitalization to develop their own business, especially banking system. Deposits, Withdrawals, transfer of money and much more processes are digitalized with advanced technologies in bank. So, it is no surprise that risks are attached to developed technology. Thus the paper will describe about threats, vulnerabilities and other cyber related issues faced by banking system in real time. However, due to the highly sensitive confidential nature of bank, this article will be limited only to the information disclosed by BSP.

Keywords: *Phishing, Spoofing, Virtual private Network, Application Programming Interface*

1. Introduction

This paper will describe our efforts in analytical interviewing the Bank of South Pacific (BSP) about cyber security issue factors such as risk, threat or any vulnerability that the enterprise could have or already faced that could affect the business functionality and how these issues are mitigated. Our questionnaires are revolved around the main question; "If the enterprise ever encountered an exploit or cyber-attack via some sort of vulnerabilities in the system".

Cyber Security is the name for the safeguards taken to avoid or reduce ant disruptions from an attack on data, computers or mobile devices. Basically they are techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitations. This report was carried out purposely to identify and analyzed about different practices that an organization enforces to secure its assets. The report compromises of fourteen questions that enquire about the organization's security measures in case of potential cyber-attacks such as viruses, malware, phishing or spoofing just to name a few.

2. The Objective of the Company

The BSP official explained the plans to recommend two-day windows to report cyber-attacks and smaller incidents, at a time of growing cases of cyber security breaches. Such reports should also release costs from theft, fraud and other incidents that may want to incur the system. The IT system needs to adopt financial firms to advance controls of digital crime and glitches and mandates the launch of 24/7 security operation centers to protect and monitor developing and highly refined cyber-threats and attacks. The main purpose/objective of the company is to provide/assist the customer to save or do their banking more conveniently.

3. Cyber- Insurance

Cyber insurance protects businesses and companies from internet-built risk and in general, the risk relating to information technology organizations and activities. The risk of nature is typically left out from the old way of doing insurance products. Handling provided by cyber-insurance policies may include first-party handling against losses such as data destruction, extortion, theft, hacking, and denial of service attacks; responsibility of handling and protecting companies or small business in losses others cause, for instance, by errors and oversights, failure to protect data or insult, and other benefits including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds.

4. Back-Up System of Companies and Small Business

The data volume that business manages, collect and store are expanding at a very rapid rate. The quick extension of data, the better you do back up of information regularly. Companies and small businesses should stage full system backups at least once at a time in a month. The backing up of the full system will make your IT system always available to protect your data from cyber threats or attacks or from data lose. Backing up data is a major way to protect your small businesses or company's progression. In an event that you backup your data on a single desktop/laptop computer or other devices like mobile etc... And it gets stolen or lost your small business or company data will be all gone. So it's best to back up every bit of data that your small business or company in different devices likes USB (Thumb) drives, External Hard Drives or places like Cloud Storage, Local Area Network (LAN) Storage, and Tape Storage. (Ward, 2019).

5. Security Checks in the Deployment Systems to Prevent Vulnerabilities

Organizations have their security check-ups built into their deployment systems to regularly monitor the system from being deployed, this comes in handy where vulnerabilities are high in the organization the system can execute both automatically and manually by IT staff. This does not eliminate all the risk but helps SME's reduce typical security risk. An example would be an Application Programming Interface (API); a set of protocols for building software applications, and Web Applications. Most businesses are using multiple web applications and APIs to streamline productivity, but they need to be checked for intruder prevention as they can easily become a back door into the network for a cybercriminal.

6. Various types of Software used to safeguard PC's

Safeguarding computers means protecting the computer's hardware from damage or theft, protecting computer systems against malware and protecting valuable data from being accessed by unauthorized personnel or stolen by disgruntled staff.

Organizations and businesses commonly utilize firewalls; a computer software program that prevents unauthorized access to or from a private network, and antivirus software such as Panda Cloud Antivirus, Bit defender, Malware bytes and Avast to immunize a computer against cyber-attacks or software that poses as a threat to your operating system. This software help secures businesses from anything that poses as a threat both offline and online.

7. Virtual Private Network (VPN)

The internet is not safe that's why the businesses need a VPN. A Virtual Private Network (VPN) is a connections method that enables security and privacy to networks – both private and public, such as Wi-Fi Hotspots and the internet. There are many reasons to why VPN is needed and used, the most popular ones are: concealing one's IP address, accessing websites blocked in a certain region, anonymity on the internet by concealing one's location, upholding the integrity of data transferred by encryption and mostly it is affordable. (What Is A VPN?, n.d.)

Basically, a VPN enables users to create a secure connection to another network over the internet.

These days VPNs are becoming popular among SMEs and large organizations. By utilizing multiple security techniques VPNs used by organizations are able to safeguard data transmissions and from access by unauthorized personals. The two main types of VPNs organizations mainly use are **Remote Access** and **Site-to-Site**. Remote access VPN uses a public network such as the internet to provide access to the organization's private network. Users will likely use a VPN gateway on their device to authenticate their identity in order to gain access to the network. Site-to-site is similar to remote access but they differ in purpose. Site-to-site connects entire networks in a geographical area to another network located in another geographical area.

Ultimately this is handy for an organization with multiple branches situated in different locations. The main reason why organizations establish VPNs is due to its security; data encryptions, mobility; resources are available to employees anywhere at any time, and cost; much more affordable than a physical private network. (Ballard, 2016).

8. Incident Response Team

Incident response teams are common in governments, organizations and businesses with valuable intellectual property. An incident response team comprises of a group of IT professionals charged with the responsibility of preparing for and responding to any form of emergency in an organization or business. The response team is tasked with developing a response plan, continuously testing it and resolving system weakness. Incident response team members are assigned different roles based on each member's technical skills in order to be prepared for future security incidents. Examples of incident response teams are:

- **Computer Security Incident Response Team (CSIRT)** is responsible for preventing and responding to security incidents
- **Computer Emergency Response Team (CERT)** is in charge of handling cyber threats and weakness within an organization
- **Security Operations Center (SOC)** is basically a command center used to monitoring, analyzing and protecting an organization from cyber-attacks. (Margaret Rouse, 2019)

9. Cyber Attack

Cyber-attack is an attempt to attack computers in order to destroy or gain unauthorized access to any information or data. There are different types of cyber-attacks that hackers use to gain unauthorized access to or destroy computers such as malware, phishing, man-in-the-middle, denial of services, and more. Cyber-attacks can cause major damages to an organization if it is successful. It can cause a financial loss in an organization, destroy an organization's reputation and relationship with its customers, and can use the organization to lose all its data. (Cyber security for business, n.d.)

Organizations do make different mistakes every day during business operations. One of the most dangerous mistakes that organizations face today is falling a victim of a cyber-attack. There are many actions that all organizations take in order to reduce the risk of cyber-attacks. Tighten your current security system, use patches, protect outbound data, use a strong password, and encrypt data are some of the actions or tips an organization should consider in order to help reduce the risk of cyber-attacks. It is best that every organization must know their vulnerabilities and know what actions to take to mitigate any risk that arises (Sadler, n.d.).

10. Recommendation

Data loss and data compromising are common threats to business operations either SME or large enterprises. Good security practice and policies could greatly help mitigate such issues when exercised properly. From the interview conducted these are just a few recommendations that are deduced (Segal, n.d.):

- Use stronger Firewalls
- Document your cyber security policies
- Plan for mobile devices
- Educate all employees on ICT and cyber security
- Enforce safe password practices
- Regularly back up all data
- Install anti-malware
- Use multifactor identification

11. Conclusion

The basis of this article is to understand the security issues that organizations like BSP face in this technological age and how to reduce such issues if they ever arise. Nowadays the cyber-attacks are highly noticeable in all the businesses. Therefore the business sectors in PNG should deploy the measures to safeguard the business from the hackers/risk. The companies can ensure the business from the cyber risk also. However, the well-trained candidates should be employed to sustain in this current business world.

Abbreviations:

API: Application Programming Interface

BSP: Bank of South Pacific

CERT: Computer Emergency Response Team

CSIRT: Computer Security Incident Response Team

LAN: Local Area Network

SME: Small and Medium Enterprise

SOC: Security Operations Center

VPN: Virtual Private Network

References

1. Ballard, B. (2016). *VPN or Virtual private network: What businesses need to know*. Retrieved from It portal: https://www.itportal.com/features/vpn-or-virtual-private-networks-what-businesses-need-to-know/.

2. Margaret Rouse, S. L. (2019, June 28). *incident response team*. Retrieved from TechTarget_Network: https://searchsecurity.techtarget.com/definition/incident-response-team.

3. Sadler, J. (n.d.). *8 Tips to Reduce the Risk of a Cyber Attack*. Retrieved from SADLER_INSURANCE: https://www.sadlerco.com/8-tips-to-reduce-the-risk-of-a-cyber-attack/.

4. Segal, C. (n.d.). *COX Blue*. Retrieved November 5, 2019, from 8 Cyber Security Best Practices For Your Small To Medium-Size_Business: https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/.

5. Ward, S. (2019, July 29). *How Successful CompaniesBackup Data*. Retrieved from

http://www.thebalancesmb.com/data-backup-is-the-best-data-protection-2947129.

6. *Cyber security for business*. (n.d.). Retrieved from NIBUSINESS: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business.

7. *What Is A VPN?* (n.d.). Retrieved from What Is My IP: https://www.whatismyip.com/what-is-a-vpn/.

8. Fineh Kevengu; Senior Analyst in Information Security, Waigani Head Office, Bank of South Pacific (BSP).

Volume 1, No.1, March-April 2020 **ISSN:** 2707-9988

Journal of ITI Centre of Internet Technologies

A Survey on Managing Cyber Security Threats, Vulnerabilities and Risks within the Royal Papua New Guinea Constabulary

Christoper Korgul[1], Cedric Robert[2], Crystal Matua[3], Manoji Maria[4], Augustine Porti[5]
[1-5]Students, Diploma in Information and Communication Technology,
School of Information and Communication Technology, International Training Institute,
Papua New Guinea, enquires@iti.ac.pg

Abstract

The growing threat of cyber-crime poses significant challenges for police department. Cyber Security plays an important role in the field of information and communication technology. Securing the data have become one of the biggest challenges in the world. Whenever a user contemplate cyber security the first thing that comes to their mind is ‘cyber-crimes’ which are growing massively day by day. Cybercrime is also called computer crime is defined as a crime in which an electronic device (i.e. computer) is the object of the crime (phishing, spamming, hacking, etc...) or is used as a tool to commit an offense (Cyber harassment, child pornography, Identity thief.)

This paper presents initial, empirical research on specialized cyber-crime units in Papua New Guinea to give an account of issues and problems faced by police staff at the frontline of cyber-policing. The article also describes the challenges due to a lack of coordination between security agencies and the critical IT infrastructure.

Keywords: *Cybercrime, Cyber Security, Vulnerability, Risk Management*

1. Introduction

The internet facility in Papua New Guinea is growing rapidly. It has given rise to opportunities in everyday field likes –business, sports, entertainment, education, and many more. It is universally true that every coin has two sides, the same for the internet both have advantages and disadvantages.

Cyber-crime is an escalating priority for national, international police and security Agencies. When it comes to Cyber security users can immediately think about how computers have influenced human’s way of living especially in business sector. The complexities of how technologies evolved also affects manual jobs since persons are replaced with machines. Computer Technologies have become very influential in the way technologies evolved, and with it comes risks or vulnerabilities. Identifying best practices to safeguard the processes and practices of the ever-increasing computer technologies is of paramount importance. This is where the main focus of Cyber Security plays a vital role.

The importance of cyber security is that it encompasses everything that relates to protecting personal information, data, confidential information, property, state and industrial systems from theft and damages by criminals. More and more devices are developed and increased with demands, so does the risks become greater. When the devices are not secured, then it poses greater risks for hackers who may have multiple portals to access the network, manipulate and steal targeted data.

The purpose of this article is to draw attention to citizens around the country about what type of cyber security risks, threats and vulnerabilities that the police department is currently facing, techniques used to prevent cybercrime and the penalties for committing cybercrime in Papua New Guinea.

2. Cyber Security Risk

Cyber security risk is the probability of a cyber-attack or data breach on your organization. Lots of organizations are becoming more vulnerable to cyber threats due to the increasing reliance on computers, networks, programs, social media, and data globally. Data breach is a common cyber-attack that have a massive negative business impact and often arise from insufficiently protected data. [1]

In light of the risk involved, cyber security protects data and the integrity of the computing assets within the organization networks. It is aimed to protect the assets against hackers or a person who behaves in a manner that is not genuine. The vulnerability of Cyber Security in Small and Medium Entrepreneur (SME) can greatly affect the business. Attacks to SME can attract direct economic costs. The cost may be incurred through;

a) Theft of corporate information
b) Disruption to trading and
c) Repair affected system, which could result in financial loss.
d) Lack of security features within an organization.

3. Cyber Security Threats

Cyber security threat is pretty nebulous — it can mean many different things depending on whom you ask. A cyber or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general or for short it is any possible danger. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks. [2]

According to research, within the Royal Papua New Guinea Constabulary, the crime investigation and IT department encounter many cyber security threats. From the operational experience, law authorization comes into contact with different digital innovations utilized for malicious and illegal means by relatively unsophisticated criminals to organized crime and local groups.

Some of the usual threats in the police IT department can include Ransomware, Malware, different types of Phishing Attacks, Social Engineering and Human error, outdated hardware and software. The reason why the Royal Papua New Guinea Constabulary encounters such cyber security threat is that still, the IT infrastructure within the country is developing.

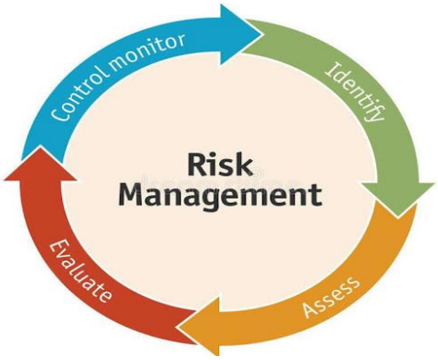
In addition, some threats to cyber security are limited to those that come through virtual attack vectors such as Social engineering Buffer overflow, Heap overflow, Stack Overflow, Format string attack, Denial of services (DoS), Keystroke logging, Screen scraping, and backdoor attack. [3]

4. Cyber Security Vulnerabilities

A vulnerability in computer security is a weakness that a threat actor, such as an intruder, may exploit to carry out unauthorized acts within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. [4]

In Royal Papua New Guinea Constabulary, there were lots of attempts that happened during the past years in order to exploit the weakness within the cybercrime investigation and information technology department-Police. The attack in the department is usually through the use of spam mail and adware.

Risk Management



Works Cited

https://www.dandmmanagementaccountants.co.uk/risk-management. (n.d.).

5. Risk Mitigation

Cybercrime and Cyber security are often misconceived to mean the same thing. Cyber security refers to “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users’ assets . In essence, Cyber security is the deterrence of Cybercrime. Cybercrime on the other hand refers to offenses committed using electronic devices, systems and or networks. [4]

Cyber Security Management is the continuous process of mitigating and preventing internal and external threats to the IT systems, equipment, and infrastructure of an enterprise to the benefit of all stakeholders who depend on these technologies. [6]

Royal Papua New Guinea Constabulary manage their IT infrastructure through;

- Encrypt data on business systems (e.g., laptops and desktops) and use strong encryption for wireless transmission.
- Separate machines that handle sensitive information (e.g., payroll or point of payment functions) from machines involved with routine services (e.g., updating Facebook and checking email).
- Provide employees access only to those systems and the specific information that is necessary to do their jobs; do not provide anyone employee access to all data or access to all systems (financial, personnel, inventory, manufacturing, etc.).
- Disable and purge old user accounts (e.g., user accounts should be disabled at the time of an employee's retirement in the department).
- Back up important confidential data on each computer used on a monthly basis and test the backups to ensure they can be read.
- Securely dispose of stored data (e.g., when disposing of old computers, remove the hard disks and destroy them; when disposing of old media, destroy any containing sensitive business or personal data).
- Deploy regularly updated firewalls, antivirus, and other Internet security solutions covering all digital devices on a network.
- Educate and train employees about cyber security (e.g., never click on a hyperlink or open a file from an unknown or untrusted source). Change any default username or passwords for computers, printers, routers, smartphones, or other devices; use strong passwords (e.g., at least eight characters long); avoid using personal information, Provide each employee with an individual account with a unique username and password.
- Keep all operating systems and software up to date (e.g., patches and updates). Avoid software from an unknown source. Remove or uninstall software that no longer is being used.
- Ensure corporate wireless networks are properly secured.

6. Cybercrime Code Act-2016

Cybercrime law in PNG was formulated and draft in the year 2011 as part of a general drive within the pacific region reform and develop the region and develop the region ICT laws. In September 2016, the parliament passed the Cybercrime Code Act. [7][8]

Cybercrime Code Act is defined by an Act or omissions constituting offenses committed through the use of Information Communication Technology (ICT) and for related purposes.

Here is some notable Section of the ACT in case of a natural person everyone should be aware of, this may include:

Sections	Threats/ Attack	Penalties
6	Unauthorized attack or hacking	Imprison for a term not exceeding 5 years or a fine not exceeding K7000 or both.
10	Data Espionage	Fine not exceeding K100, 000 or Imprison for a term not exceeding 30 years.
15	Identity thief	Fine not exceeding K15000 or Imprison for a term not exceeding 10 years or both.
17	Pornography	Imprison for a term not exceeding 15 years or a fine not exceeding K25000 or both.
23	Cyber harassment	Imprison for a term not exceeding 7 years
27	Cyber Attack	Imprison for a term not exceeding 15 years or a fine not exceeding k50,000 or both

Works Cited

Parliament, N. (2016). Papua New Guinea *Cybercrime Code Act 2016.*

7. Conclusion

Cyber Security is a key function within the body of computer technologies and networks. Maintaining the efficiency of effective cyber security practices that can protect vital data which is the primary objective of any organization, be it government or industrial. Therefore, there is no perfect solution for cyber-crimes but users should try their level best to minimize them in order to have a safe and secure future in cyber space and Cyber Security is an important function in Information and Communication Technology (ICT).

References

1. Choi, K.-S. (2016). Ransomware Against Police: Diagnosis of Risk Factors via Application of. *International Journal of Forensic Science & Pathology (IJFP)*, 254.

2. Kingori, D. (2019). https://www.uscybersecurity.net/writer/duncan-kingori/. Retrieved from https://www.uscybersecurity.net

3. Rajini Goel, J. H., & Kumar, A. (2018). *Managing Cybersecurity Risk in Government: An Implementation Model*. Washington DC 20059: ibM Center for the business of government.

4. Tunggal, A. T. (2019). *Cybersecurity: What Is Cybersecurity Risk? A Thorough Definition*. Retrieved from UpGuard: https://www.upguard.com/blog/cybersecurity-risk

5. Whitman. (2004). *Managing Cybersecurity Threats*. Retrieved from KB Manage: https://www.kbmanage.com/concept/managing-cyber-security-threats

6. Wong, A. (2016). *Cyber Security: Threats Challenges Opportunities*. Retrieved from www.acs.org.au

7. Parliment, N. (2016). *Cybercrime Code Act 2016*. POM: PNG Government. http://www.parliament.gov.pg/uploads/acts/16A_35.pdf

8. https://www.dreamstime.com/stockillustration-risk-management-businessdiagram elements-safety-vector-version-available-image55728250

Volume 1, No.1, March-April 2020 **ISSN: 2707-9988**
Journal of ITI Centre of Internet Technologies

Risk, Threats and Vulnerability of Cyber-Crimes in SME in Papua New Guinea

Brown Maiwax[1], Mary Agua[2], Yuriel Bomai[3], Shaney Toinevane[4]
[1-4]Students, Diploma in Information and Communication Technology,
School of Information and Communication Technology, International Training Institute,
Papua New Guinea, enquires@iti.ac.pg

Abstract

Cyber threats are the possible dangers of malicious attempts to damage a network of computers. This paper focuses on the security management issues of Papua New Guinea (PNG) Dataco. Dataco was established as part of the Government's plan to restructure and transform the Telecommunication Industry in PNG. It is a state-owned wholesale enterprise that provides only ICT services. In providing faster internet and better connectivity, more opportunities are open up in the digital economy, which can also be a great advantage for a cyber-activity that is illegal and can be vulnerable. With that, it's essential to understood the concept of using the introduced technologies with 4G internet.

Keyword: *Cyber Security, Risk, Threat, Vulnerability*

1. Introduction

Every year, 43% of Cyber-attacks targets small businesses while ransomware is increasing. With 43% of online attacks now aimed at small businesses, a favorite of high-tech millions, get only 14% prepared to defend themselves, Owners need to give more priority on high tech security to protect from any cyber -attacks.

Nowadays, digital transformation cyber-crime has become one of the fastest-growing forms of criminal activities. Equally worrying for modern executives, it's also set to cost businesses $5.2 trillion worldwide within five years, according to Accenture. The average cost of cybercrime for a company has increased from $1.4 million over the years, to $13 million and the average number of security breaches rose by 11% from 130 to 145.

Risk is the likelihood of a cyber-attack or data breach on a computer system in an organization. To control risks, consider strengthening network security and privacy settings. Threats, on the other hand, refers to whatever that has the potential to cause severe harm to a computer system. Threats are something that could or could not occur but have the potential to cause serious damage.

The more the security systems of networks are weak; the chances of cyber vulnerabilities are greater. Vulnerability is a cyber-security term that refers to a weakness in a system that can expose to attack. It may also refer to any type of flaw in a computer system itself, in a set of events, or anything that leaves information security exposed to a threat as well as risks. The paper basically refers to a study done in PNG Datacom about its general operation, likely cyber threats or risk, vulnerabilities and how it should be managed.

2. General Operation

DataCo provides affordable high-speed wholesale internet transmission capacity to retail ICT service providers.

DataCo's core business is focused on three (3) core market segments.

1. PNG Fixed/Broadband Operators

Dataco will serve the needs of fixed voice and broadband service providers based on the population that they will benefit from purchasing domestic and international transmission services from DataCo. This would enable Telikom to re-direct capital to other parts of its network. (“Last mile”) that connects directly to retail customers and front line service, which would enable Telikom to differentiate itself in the market. DataCo will provide Internet Service Providers (ISP) with customized service offerings, including “Pay as you grow” constructs to stimulate demand and de-risk market entry for new ISPs.

2. PNG Mobile Network Operators (MNOs)
DataCo proposes to provide cost-effective, reliable and scalable transmission services from major PNG centers to their mobile switching centers (MSCs) and International gateways. DataCo with its suite of wholesale transmission services around the country can maximize their respective return on investment cases and lower the cost of expanding their network coverage as well as meeting the increased demand for backhaul transmission capacity required when they deploy new 3G and 4G mobile technologies.

3. Internal Carriers
DataCo will offer connectivity to International carriers such as Southern Cross Cable Network and provide seamless International and domestic capacity at bundled prices that will serve to stimulate competition in the local and international markets.

3. Common Threats usually faced by SMEs

3.1 Internal Attacks

The Internal attack is one of the current largest cyber security threats faced by (Small and Medium Enterprises) SMEs. Rogue employees, especially those who are with access to the network, sensitive data or admin account is capable of causing real damage *(Fig: 1)*.

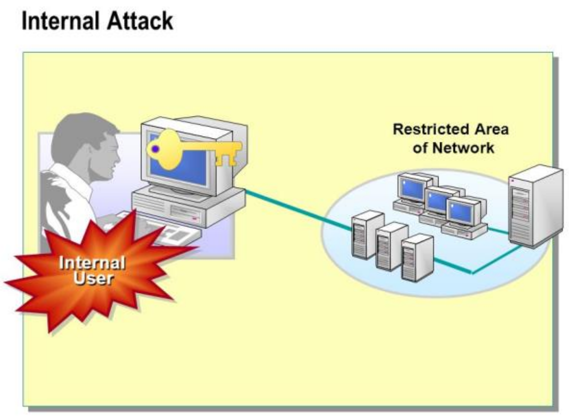


Figure: 1Internal Attack

(Cited: https://slideplayer.com/slide/5775510/)

3.1.1 Risk Reduction

- Identifying privileged accounts- accounts with the ability to significantly affect or access internal systems.
- Implement tools to track the activity of privileged accounts.
- Terminate those that are no longer in use or are connected with an employee no longer working in the business.

3.2 Phishing

What’s the catch of the day?

Phishing is one of the fraudulent methods are used by criminals to gain the personal, private data of the businesses.

3.2.1 Spear Phishing

Spear Phishing is a target form of phishing emails. They are designed to appear to originate from someone who knows and trust such as a senior manager. Cyber criminals can study the social media of those with access to privileged accounts to gain insight into the use of their phishing emails appears authentic. If an employee is tricked by a malicious link in a phishing email, they might unleash a ransom attack on small businesses.

3.2.2 Risk Mitigation of Phishing and Ransomware

Because of ransomware permanently lockdown files, businesses should ensure securing backups of their critical data.

Organization ensuring staff to be fully aware of the dangers and know how to identify a phishing email.

3.3 Lack of Cyber Security Knowledge

Cyber Security strategies, policies, and technologies are worthless in an organization if an employee lacks cyber security awareness. Education and training are essential to reduce the risk of cybercrime. Some employees may not be able to care enough to protect themselves online which can put a business at risk.

- Training sessions must be taken to help employees manage passwords and identify phishing attempts.
- Provide support to ensure an employee has the resources, needed to be secure.

3.4 Distributive Denial of Services (DDOS) attack

This occurs when a website is flooded with more traffic than it can handle. It can damage the company's financial stability and reputation.

If the business relies on online services such as websites to function, the outage caused by DDOS attacks will be catastrophic.

3.4.1 Attack Reduction

- Businesses can't stop a service being targeted in a DDOS attack, instead, they can work to absorb some of the increased traffic, with more time to form a response.
- Ensure there is extra bandwidth available and creating a DDOS response plan in the attack event or using a DDOS mitigation service.

3.5 Malware

Malware refers to any file or program used to harm a computer user such as worms, ransomware, computer viruses, Trojan horses, spyware and others.

3.5.1 Malware Prevention in Businesses

- Investment in solid antivirus technology, system software, firewalls, and firmware must all be kept up to date. If the software is not updated, they are at a serious risk.

Figure: 2 The Crib Sheet A-Z (Virus, Malware and More)

3.6 SQL Injection

Structured Query Language (SQL) injection refers to vulnerabilities that allow hackers to steal sensitive information left behind a web application by sending malicious SQL commands to the data server through code inputs into forms. In operation, many businesses rely on websites and many entirely depend on the service they provide online. If the websites are not properly secured, cyber criminals could have engaged in data theft.

3.6.1 Protection of SQL Injection

- The business should assume all user-submitted data is malicious so get rid of database functionality that is not needed and considering a web application firewall.

Figure: 3 SQL Injection

3.7 BYOD (Bring Your Own Device)

If employees are using their mobile devices that is unsecured to share or access company data, business is vulnerable to data theft. They could carry malicious application which could bypass security and access the company's network.

3.7.1 Solution

- Placing a BYOD defined policy. Educates employees and on-device expectations and allows companies to better monitor downloaded email and documents to the company's devices.
- Ensure the devices owned by the employee to access the business network through (VPN) virtual private network which connects remote BYOD users with the organization via an encrypted channel.

3.7.1.1 Security Software used

In general, there are numerous good security software's available in the technological market depending on the level of security required by organizations to protect the business data from cyber threats.

The company (DataCo) would recommend LMNTRIX because it provides adaptive threat response solutions apart from other security software like Symantec, Microsoft Security Essentials, Kaspersky *(Fig:3)* and many more.

3.7.1.2 Data Backup

The company does data backup and retention daily, weekly, as well as monthly. Primarily it depends on the type of data and the criticality of the system being backed up.

3.7.1.3 Security Training

Security training is paramount. The company makes sure every security training is attended every year depending on the availability of the course and the schedule.

True Cybersecurity for Business

by Kaspersky Lab

True Cybersecurity does not just prevent cyber security incidents: it predicts, detects and responds to them – effectively, flexibly and reliably.

Figure: 4 Kaspersky Screen

3.7.1.4 Risk Management Strategy

The most common risk management strategy used by the company *(Fig: 5)* is labeled below.

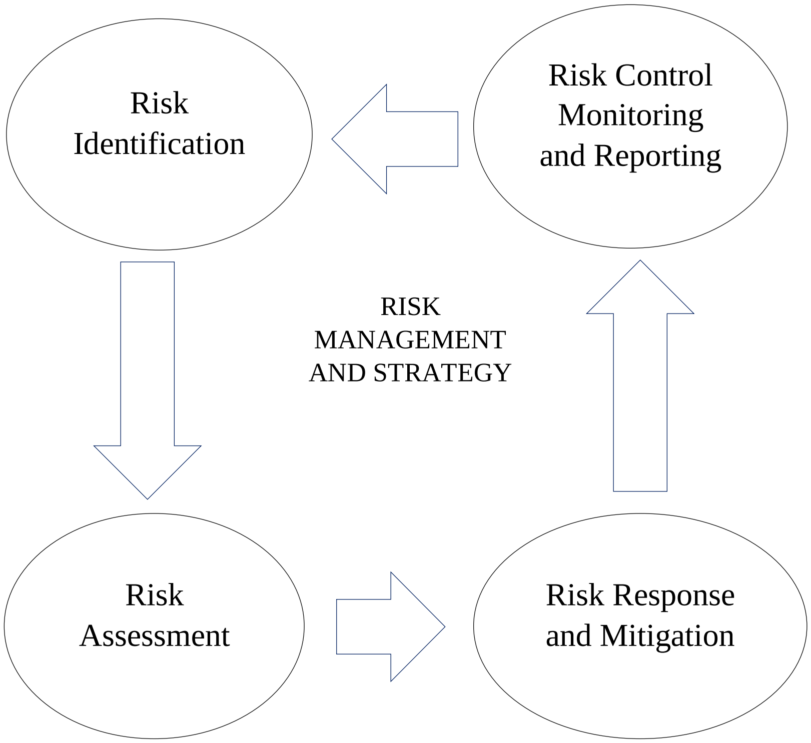

Risk Identification
Risk Control Monitoring and Reporting
RISK MANAGEMENT AND STRATEGY
Risk Assessment
Risk Response and Mitigation

Figure: 5 Risk Management Strategy

4. Conclusion

Cyber security has become a seal on the battlefield of Small and Medium Enterprises. It is the daily guide for every operation within the organization. Cyber security protects the assets of an organization from the hacker's theft or an attacker with the intention of causing damages. In PNG most SMEs are not considering security into account that is because serious cyber-attack has not faced, yet, the new threats are developing every now and then which could lead to unexpected attack so its recommended that security will offer a comprehensive solution to protect against a diverse range of issues. Investment in Cyber Security will protect or secure your business, increased productivity, inspire customer confidence, customer protection, stopping web sites from falling.

Abbreviations:

BYOD: Bring Your Own Device

DDOS: Distributive Denial of Services

MNO: Mobile Network Operators

SME: Small and Medium Enterprises

SQL: Structure Query Language

References

1. Amrin, N. (2014). *The Impact of Cyber Security*. Retrieved from University of Twente: https://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf
2. Freire, E. (2016, September 22). *Guidance on cyber resilience for financial*. Retrieved from Committee on Payments and Market Infrastructures: http://pubdocs.worldbank.org/en/987101479484759693/GPW2016-thur-Freire-Cyber-Guidance.pdf
3. Cyber Security Policy Division, D. o. (2019, November). *BSA Comments on Australia's Cyber Security Strategy*. Retrieved from The Software Alliance-BSA: https://www.bsa.org/files/policy-filings/11012019au2020cybersecuritystrat.pdf
4. MARSH, M. (2019, September). *2019 Global Cyber Risk Perception Survey*. Retrieved from Microsoft: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf
5. Ombudsman, Australia. (2017, 09). *www.asbfeo.gov.au*. Retrieved from Australian Small Business and Family Enterprise Ombudsman : https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-research-report.pdf
6. https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html.
7. https://www.slideshare.net/ifad/2-project-risk-management