NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

CE/CZ4064 Security Management Project Report

Group: P5G4

Project Title: The new normal in managing security

Group Members:

Name	Matriculation Number
Goh Hong Xiang, Bryan	U1920609E
Lee Cheng Han	U1920206L
Chua Chong Hung Melvin	U1921924G
Chua Chong Wei Kelvin	U1920206L
Lee Jun Hong Eric	U1820995G
Chong Jing Hong	U1922300B

Table of Contents

Introduction 3

Bringing Sensitive Work Materials Home 3

Remote Meetings 5

Weak Financial Capability in Start-Ups 7

Conclusion 9

References 10

Introduction

With the Covid-19 pandemic, governments around the world have implemented pandemic measures and lockdown procedures, forcing many companies and start-ups to change their work practices from in office work life to remote work in order to adhere to covid-19 rules and regulations from the government. With a change in work styles / culture there will definitely be new vulnerabilities introduced.

Bringing Sensitive Work Materials Home

Vulnerabilities

Firstly, due to the increase in work-from-home practices, attack surface increases. Thus, there are new attack vectors such as home routers, home network and home computers (The Straits Times, 2021). For example, home routers could be exploited by DNS hijacking where hackers can breach the security of your home Wi-Fi and potentially steal confidential information by redirecting users to malicious websites.

Secondly, with most business employees working from home, there will be lapses in keeping sensitive and confidential work information secure. One can fall prey to the prying eyes of their family members such as young children (Kaspersky, n.d.), who may not understand the concept of confidentiality. Confidential information could be leaked, which could cause data breaches.

Lastly, there is an increase in the usage of work devices for personal use, hence, employees are now more vulnerable to phishing attacks. A study by HP Inc. (HP Wolf Security, 2021) finds that 70% of office workers use their work devices for their personal use, 69% are using their personal laptops or printers for work-related use and 30% of remote workers have let someone else use their work devices. Titled ‘Blurred Lines & Blindspots’, the report also reveals other damning statistics:

- 33% download more from the internet than prior to the pandemic – a figure that rises to 60% for those aged 18-24.
- 27% of respondents use their work device to play games more than prior to the pandemic – a figure rises to 43% for parents of children aged 5-16.
- 36% use their work device for watching online streaming services – again, this figure rises to 60% among those aged 18-24.
- 4 in 10 office workers admit to using their work device for homework and online learning more in the past year. This figure rises to 57% for parents of children aged 5-16.

Hackers are aware of these patterns and are exploiting them for their phishing campaigns. According to KuppingerCole, there was a 54% increase in phishing activities by malicious actors in gaming platforms. They also found at least 700 fraudulent websites impersonating popular streaming services in just one 7-day period in April 2020 (HP Wolf Security, 2021).

HP Wolf Security's threat insights also showed an increase in gaming-themed malware. For example, campaigns have been found distributing Ryuk ransomware via file sharing websites and samples of stealthy JavaScript downloader malware. Users were also found attempting to download malware-infected files from their personal email accounts to their work devices.

Risks Management

Due to the work from home setting, staff have to pay more attention to cybersecurity threats themselves. Vulnerabilities such as the internet, home routers, passwords and home computers can be exploited by hackers, thus, it is of utmost importance to increase cybersecurity at home (Mooney, 2020).

Firstly, workers can install and use a Virtual Private Network (VPN) on their computer. A virtual private network encrypts all of your internet traffic, making it unreadable to anyone who intercepts it. Hence, employees should exclusively use the VPN when working and when accessing company information systems remotely.

Secondly, the passwords of home routers should be changed regularly. Employees should also ensure firmware updates are installed so that security vulnerabilities can be patched.

Thirdly, workers should have a strong password and always use two-factor authentication. Two-factor authentication acts as an additional layer of protection to an employee's accounts. The authentication method could be an email or text message confirmation, or a biometric method such as facial recognition or a fingerprint scan. Two-factor Authentication can only be bypassed if the hackers have access to the worker's phone or email. Therefore, It is a strong measure to increase the cybersecurity at home and prevent family members from leaking confidential information.
In addition, backups are also an important measure to increase security at home. All important files should be backed up regularly so that in case of ransomware, the lost files can be restored from the backups. One of the most convenient and cost-effective ways to back up files is through the cloud.

Using firewalls and antivirus software can increase security at home. Firewalls act as a first line of defense to prevent threats from entering your home devices. They create a barrier between employees' devices and the internet by closing ports to communication. This can prevent malicious programs from entering and stop data leaks from employees' devices. Although a firewall is a good layer of defense, threats will inevitably get through. An advanced antivirus software can act as the next line of defense by detecting and removing known malware. Even if malware does manage to find its way onto an employee's device, an antivirus may be able to remove it.

To address phishing vulnerabilities, businesses can deploy the Responsive Security Approach. The main motivation behind this approach is to recognize that weak links are inevitable and we can only reduce the impact of the risks. It uses a combination of social-technical tools and methodologies to implement and maintain an information security program. In this regard, businesses can conduct anti-phishing campaigns to raise employee's awareness to potential spear phishing threats through email.

Measuring Success

Following the anti-phishing training, the cyber security department can conduct tests to evaluate employees' awareness of phishing emails. The tests could involve sending emails just like other ordinary emails to employees. Employees that clicked on the email will send a notification to the department. Over time, from the statistics collected, businesses can measure the success of their own campaign.

There are 3 main metrics that can be used to measure the success of a phishing campaign: open rate, click rate and report rate (Lewis, 2020).
Open rate is the percentage of recipients who opened the phishing test email. This metric tells us if the email was enticing enough for someone to open it. Open rate is influenced by the information that is seen exclusively in the inbox, such as subject line, send email address and name etc.

Click rate is the percentage of recipients who clicked on the phishing link inside the email. This is the most common metric which the training provider will look at as clicking on it will mean that the employee had failed the test.

Report rate is the percentage of recipients that reported the phishing email to their IT support team. Report rate is the most important metric. This is because correctly identifying a phishing email and deleting it is beneficial to the recipient alone, whereas correctly identifying a phishing email and reporting it can make others aware.

Remote Meetings

With the rise of Covid-19 cases, companies are encouraged to pivot towards remote work and this has remained the de facto norm throughout the last 2 years. This has led to the meteoric rise in demand for remote meetings tools. In particular, Zoom has been one of the most popular tools since the onset of Covid-19 due to its ease of use and installation coupled with their freemium-pricing model. This sharp unexpected increase in user demand has exposed multiple security issues that have plagued Zoom (BBC, 2020).

Vulnerabilities

One of the notable vulnerabilities that have emerged is “Zoom-bombing”. It is a type of cyber harassment where an unwanted individual tabs into someone else’s private meeting (Wikipedia, n.d.). Depending on the content of that meeting, consequences may range from plain nuisance to severe. Nonetheless “Zoom-bombing” has indeed become an issue and remains an important information security risk.

Due to the multifold increase in remote meetings, a simple search on Google or simply guessing the nine digit ID code can return multiple links to private meetings (Bernstein, n.d.). Furthermore, Zoom reuses meeting IDs and some meetings do not require any password to access. This oversight allows playful individuals or intentional infiltrators to access the meetings without the need for authentication leading to many disruptive incidents that can be offensive or embarrassing, eg. circulating pornography or racist material, disruptive behaviour. This can also pose severe consequences to involved parties. For example, if key confidential data was leaked due to an unauthorized individual tapping into the remote meeting, it could result in major financial losses. Furthermore, a real life incident concerning UK’s Prime Minister Boris Johnson, who accidentally tweeted a picture containing the ID number of their congressional meeting, highlighted the vulnerabilities and risk that users face (Press Association / thejournal.ie, n.d.).

Risk Management

Zoom’s CEO has pledged to address these key concerns by generating new random meeting IDs and lengthening passwords. However, companies on their end should classify their meeting sessions based on information security classifications and limit the usage of Zoom to unrestricted information sharing like Scrum meetings. For important meetings that involve trade secrets, they should limit communications to secure applications such as Signal/in-house applications that offer best in the business end-to-end encryption and security. In spite of this, all communication platforms will inevitably present a certain degree of threat and vulnerability. Therefore, companies can continue to enhance and manage the security risk of Zoom through a series of carefully crafted security risk policies such as:

1. **Trust but verify** people attending the meeting through secure login verification with their associated credentials and ensuring that no unauthorized personnel is attending the meeting.

2. **Secure the meeting room** with a unique meeting ID and password for all calls.
3. **Enforce updating applications** to enjoy the newest updates and security options presented to them.

Due to the nature of service Zoom provides, we should implement a responsive risk based approach. This is because it will be near impossible to detect the infiltration until it has already happened. Zoom should remain vigilant and responsive by:

1. Being aware of visible change in events
2. Situation awareness upon detection of significant changes
3. Critical alignment responds to re-align critical assets, people, infrastructure, and/or processes (both technical and social) to the new situation

Responsive security approach uses a combination of social-technical tools and methodologies to implement and maintain an information security program. The social aspect focuses on the "soft" issues, i.e., human activities related challenges, whereas the technical aspect focuses on the "hard" (technical or engineering related) challenges.

Measuring Success

Due to the nature of this security risk, it is hard to measure success of the strategies proposed quantitatively based on outcomes/number of attacks prevented. This is because if a malicious Zoom-bombing attempt happens, it will be near impossible to detect the infiltration.

However, we can best measure the success of these policies through an assessment of the level of preparedness of employees. This is because most of the policies proposed address human error, non-compliance or ignorance. Security awareness training quizzes can be issued to make sure that employees are well informed and up to date with the best practices they can follow to protect the organisation. Another metrics would be responsiveness and time of remediation. Responsiveness is key as vulnerabilities have to be addressed as soon as the infiltration is detected and time of remediation would depend on the type of approach be it 'soft' or 'hard'.

Weak Financial Capability in Start-Ups

Given the current pandemic situation, many companies have been adversely affected and start-ups are not spared. In fact, they are hit worse as compared to the rest (Asheem Chandna, 2020). This is mainly due to weak financial capabilities that a typical start-up possesses.

Vulnerabilities

Due to COVID-19, many companies that are trying to enter various industries face many difficulties. Demand has also dropped sharply for most new companies and the report states that 72% of startups saw their revenue decline since the start of the crisis while the average startup experienced a revenue decline of 32% (McCarthy, N., 2020).

The decrease in revenue will worsen their financial capability. Due to the worsening financial capability, Startups would be more unwilling to spend on crucial software to enforce their security. Not only that, startups would be forced to hire short term employees such as interns or people with weak cyber security knowledge. This would result in more lapses in security measures, introducing new attack surfaces and new attack vectors for cyber-criminals to exploit.

Risk Management

With the very weak financial capability that a startup has, they have to be very prudent in how they fortify their security through efficient management of their security.

1. **Threat Analysis**

   Before an organisation develops solutions to protect itself, it is imperative for them to first understand their threats in order to prioritize which attack surfaces to protect. Firstly, they have to identify its attack surfaces and potential attack vectors. Following that, they would determine their severity and likelihood of each occurrence. They can use Fault tree analysis to have a top-down view of their system's reliability and vulnerabilities. Event tree analysis can be used to determine the potential threats through the success/failures of various subsequent events.

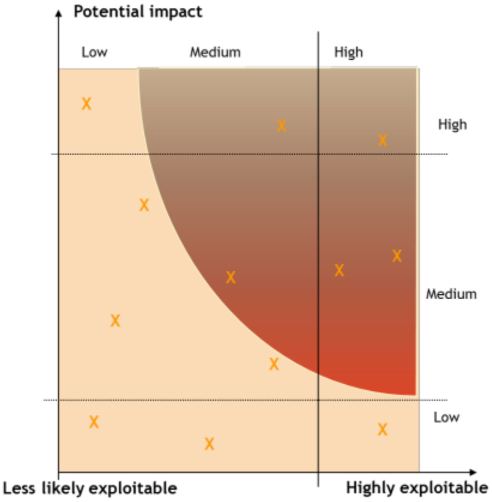

Figure 1. 2D matrix

   Risk assessment can then be performed by calculating each event's Risk Probability Number (RPN = probability * detectability * severity). They can then plot a 2D matrix as shown above in figure 1. From the matrix, they can decide which risk to accept, to reduce and which to remove. Through this, they can manage their spending more efficiently by prioritizing which threats to protect first.

2. **Culture**

   It is imperative to create a culture where employees are motivated to identify security incidents and report them without worrying about the consequences. In traditional workplaces, some employees may not report these lapses as there may be negative consequences and would want to cover up the security incident. Therefore, empowering employees is important, even more especially in small startups as this would reduce the number of security incidents and would save costs.

Measuring success

Using threat analysis, we can measure the level of success of the policy through the following metrics.

Startups can compare the amount of investment to the benefits derived. These benefits can be quantified by the amount of savings resulted year on year by calculating the total amount spent for incidents and investigations. If the amount of benefit increases over the years, this goes to show that the security of the system is better as there would be less incidents.

Another way for them to measure is through the amount of time spent (usually in number of days) to resolve or investigate these incidents. The amount of time spent on these solutions can be a metric to gauge the performance of the strategy.

Conclusion

From the aforementioned discussions, it is in businesses best interest to practise good security management to prevent occurences of security lapses. Companies should invest in good security measures even though they may be costly. This is because the losses incurred from potential attacks are far more costly. One need not look far back to see the amount of damages businesses can incur. The data breach of Target in 2013 resulted in a $290 million loss (Manworren et al., 2016).

According to a research in 2018, the average cost per record lost in a data breach is $148 and the average total cost of a breach is $3.86 million. Even a small business with 1,000 lost records could see costs in the tens of thousands (Juliana, n.d.).
Data breaches can also see reputational losses for businesses as customers lose confidence in the company’s brand, resulting in a drop in revenue. These statistics show that having a solid security system is a worthwhile investment.

References

Asheem Chandna. (2020, july 22). *Covid-19’s Impact On Startups: Assessing The First Few Months*. Covid-19’s Impact On Startups: Assessing The First Few Months. https://www.forbes.com/sites/asheemchandna/2020/07/22/greylock-covid-19-impact-on-start-ups-assessing-the-first-few-months/?sh=5c5d84521c8f

BBC. (2020, April 2). *Zoom Boss apologises for security issues and promises fixes*. BBC. https://www.bbc.com/news/technology-52133349

Bernstein, C. (n.d.). *What is Zoombombing?* https://searchsecurity.techtarget.com/definition/Zoombombing?_gl=1*xrbvnz*_ga*OTY3MDI2MDA3LjE2MzA1Njg4MjI.*_ga_TQKE4GS5P9*MTYzMDU2ODgyMi4xLjAuMTYzMDU2ODgyMi4w&_ga=2.180111588.1340989820.1630568822-967026007.1630568822

HP Wolf Security. (2021, May 12). *Announcing HP Wolf Security, and a New Report Assessing Remote Working Cyber Risks*. Announcing HP Wolf Security, and a New Report Assessing Remote Working Cyber Risks. https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/

Juliana, G. D. (n.d.). *The History of Data Breaches*. The History of Data Breaches. https://digitalguardian.com/blog/history-data-breaches

Kaspersky. (n.d.). *Cyber Security Risks: Best Practices for Working from Home and Remotely*. Remote working security risks & tips | Kaspersky. https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe

Lewis, J. (2020, August 6). *How to measure a phishing test program*. Cira. Retrieved October 24, 2021, from https://www.cira.ca/blog/cybersecurity/phishing-test-metrics-measurement

Manworren, N., Letwat, J., & Daily, O. (2016). Business Horizons. *Why you should care about the Target data breach*, *59*(3), 10. https://www.sciencedirect.com/science/article/pii/S0007681316000033?via%3Dihub

McCarthy, N. (2020, June 29). *How Covid-19 Has Impacted The Global Startup Scene*. Forbes. https://www.forbes.com/sites/niallmccarthy/2020/06/29/how-covid-19-has-impacted-the-global-startup-scene-infographic/?sh=30c636015a7e

Mooney, S. (2020, August 20). *Cyber Security Tips for Allowing Employees to Work From Home*. Cybereason. https://www.cybereason.com/blog/cyber-security-tips-for-allowing-employees-to-work-from-home

Press Association / thejournal.ie. (n.d.). *Boris Johnson tweet of virtual Cabinet raises cybersecurity concerns*. https://www.thejournal.ie/boris-johnson-tweet-of-virtual-cabinet-raises-cybersecurity-concerns-5063195-Mar2020/

The Straits Times. (2021, July 7). Working from home amid Covid-19 pandemic blamed for rise in cyber hits on Singapore organisations. *The Straits Times*. https://www.straitstimes.com/tech/tech-news/working-from-home-amid-covid-19-blamed-for-rise-in-cyber-hits-on-singapore

Wikipedia. (n.d.). *Zoombombing*. https://en.wikipedia.org/wiki/Zoombombing