Vertical Institute

Capstone Project

Security Risk and Recommendation

Mui Gek Tan _ Capstone Project

TABLE OF CONTENTS

03 Incident Response Management for Ramsomware attack

Incident Identification

Incident Categorization

Incident Response Team

Incident Plan

Executive Summary

The banking and financial sector is uniquely exposed to cyber risk. Our firms—given the large amounts of sensitive data and transactions we handle—are often targeted by criminals seeking to steal money or disrupt economic activity. Attacks on financial firms account for nearly one-fifth of the total, of which the bank are the most exposed.

In recent years, there has been a significant uptick in the frequency and sophistication of attack to the branch of our bank in Singapore, A new variant of phishing scams using spoofed SMS messages to target employee in our various brach has been making its rounds, say the CEO from OBC Bank. It contributed to 374 reported cases involving losses totalling about $1.07 million between January and May this year.

Another high profile Cyber Attack **Ransomware Attack**, are expected to climb amid rapid digitalisation. In 2021, Ransomware attack were up to 54 per cent compare to 2021 in back and financial industries. This malicious software would lock up digital systems until a ransom is paid to the hacker.

Risk and Recommendation

Risk 1: Phishing Attack

Phishing Attack is a cybercrime in which hacker try to lure ones into giving out their personal information by impersonating a legitimate authorize user to trick employees giving out their credential with one time password.

Base on the statistic in 2022, our employees hit by the Phishing attack has increase with 2,000 reported cases in 2021, more than twice reported cases in 2020. They have either open the link or attachment with the company email without knowing that these are phishing email attack.

As a result, a total of $350,000 have loss, with the larger amount of lost was $20,000, and the lower amount of lost was $50.00.

Recommendation 1

Defense in depth

1. Multiple layers of security to stop the attacks from going through
2. Password + Multi-factor authentication
3. Firewall + Anti-virus
4. All of the aforementioned working in unison

Due to the sophisticated technologies we are having today, it would not be sufficient to just reply on a single protective measure. That why it is important to implement the **Defense in depth** into all our branch. **Defense in depth** is a cybersecurity approach that can protect our employees under several layers of security protocols, so if one mechanism fail, another step up immediately to thwart the attack.

Recommendation 2

Issue Security Newsletter to employees that teach them how to identify fake link and malicious email

Issue Security Newsletter to employees to keep them up-to-date for the cyber security news, cyber-attacks and vulnerabilities, and security awareness tips and stories. This can allow employees to gain Industry insights, timely threat alerts, so to enjoy a more safer cyber world on the internet.

CYBERSECURITY AWARENESS MONTH

Do your part. #BeCyberSmart.

#BadJokes for Cyber Folks

Bad jokes can be so good. Enjoy a fun take on a serious topic with our best #BadJokes about cybersecurity.

Why did the chicken cross the node? To get to the endpoint on the other side.

Have you heard about the new Camo malware? It's really hard to detect.

A laptop and a desktop walk into an empty bar. The desktop sits down at a table. The laptop looks around angrily and shouts, "Where am I supposed to sit?!"

Did you hear about the man who used the factory password on his router? When his network got hacked, he got all the blame by default.

My friend has a real problem. She just can't stop herself from clicking on phishing emails. She's hooked!

When I was a kid, we used to worry about acid rain. With everything being uploaded to clouds nowadays, it's only a matter of time before we'll find ourselves drenched in data.

Don't be aware, be smart

At a time when we are more connected than ever, to say that practicing good digital hygiene is important would be a massive understatement.

Increasingly sophisticated cyberattacks and constantly evolving cybercriminals make daily attention to risk mitigation imperative. **It's not enough to be "cyber aware" anymore. Today, you must #BeCyberSmart.**

Each new connected device you use and online account you establish increases your attack surface and provides cybercriminals with another potential point of entry. And yet, the consistent practice of cybersecurity basics remains the most fundamental way to protect yourself and others.

Any device that connects to the internet is vulnerable to risks. **If you connect it, protect it.** The best defense is to keep your device's software, browser and operating system up to date.

#BeCyberSmart Tip: *When appropriate, turn on auto-updates.*

Pas$w0rds_d0n't_hav3_2_b_th!s_ComplicateD! **Use a phrase** to create a lengthy, unique and memorable password.

#BeCyberSmart Tip: *There's no one like you in the whole world - except a cybercriminal with your password. Don't get hacked. Use multi-factor authentication (MFA).*

Common sense plays a substantial role in maintaining good online hygiene. **Do your research before downloading new software or apps.** Consider the publisher's reputation, including user reviews and published articles.

#BeCyberSmart Tip: *Just because you don't use the software or app you installed doesn't mean that it's not using your device. Delete unused software/apps to increase the device's available space and reduce your attack surface. Win-win.*

Be diligent about **privacy and security settings,** including who can access your documents and devices. Take a few minutes to configure these settings before using new devices or accounts, and periodically revisit them to address possible changes.

#BeCyberSmart Tip: *For web meetings, require a password so only those invited can attend, and restrict screen and file sharing by attendees.*

No single tip is foolproof, but practicing them in parallel is the best way to maintain good online hygiene and protect yourself, and the people and networks with whom you connect, from cyberattacks.

Risk 2: Ransomware Attack

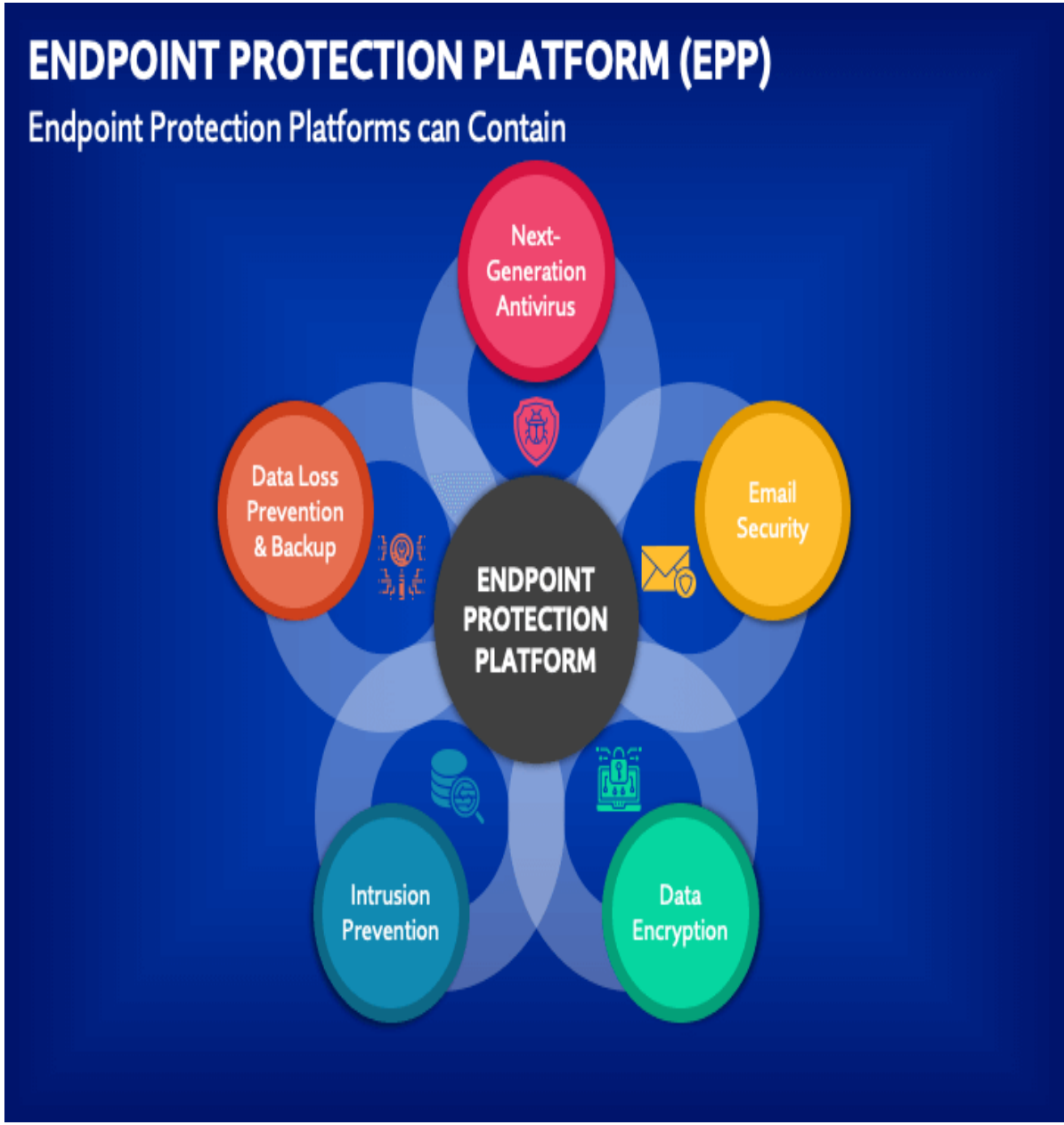
Ransomware Attack is a type of malware that been taken over of the accounts and sensitive data exposure from our employees. In 2021, there are cases that Ransomware attack that affacted 5 laptop at our branch at Ang Mo Kio, the personal data of about 129,000 were stolen by hackers during the ransomware attack. As a result, it cost disruption to our operation as we need to shut down our branch for 4 days, thus it suffers a total of S$50,000 potential turnover.

Recommendation 1:

Build Email Protections and Endpoint Protections

To educate employees not to open unknow emails, or unfamiliar link.
Make it an appoint to Scan all emails for known malware strains, and keep firewalls and endpoint protections up to date with the latest known malware signatures.

To enhance the protection against cyber-attacks, our organization also upgrade a
Stronger anti-virus protect with $25,000 per year.



Recommendation 2:

Regular Backup

To prevent of the data due to the Ransomware attack, company have introduce the **cloud backup** for email that automatically syncs up to six time per day**.**

Backups and recovery should be verified daily. If any errors found during the backup, it should be solve them, as we never know when the next disaster or ransomware will occur.

Incident Response Management for Ransomware

From the statistic shown, as well as a cyber-attack outbreak in one of our branch in 2022, up to 20 percent of all cybersecurity breaches are ransomware attacks, so it is very critical for the organization to have a Incident Response Management for Ransomware, so to have an immediate disaster recovery from any cyber-attack.

Incident identification:

- Suspicious changes to files, file names, or locations
- The installation of unauthorized software, as attackers install various tools, such as Mimikatz, to help them exploit vulnerabilities, and carry out other relevant tasks.

Incident Categorization

- Determine which systems were impacted, and immediately isolate them.
- Power down the system if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.
- Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.

Incident Response Team

Incident response team with a group of IT professionals is activate during the time of cyber-attack.

- **Incident manager.** Leads and coordinates all incident response activities **(communication, investigation, containment, recovery)**. He is also the one who makes critical decisions on resource allocation, prioritization, escalation procedures.

- **Technical team.** IT, security team members and other employees with technical expertise across company systems. The technical team will be the core of the overall incident response team, and should include security analysts and threat intelligence.

- **Communications coordinators.** Responsible for managing internal communications Relating to incident response efforts, as well as public relation representatives to Manage relationships with media outlets, affiliated business entities and extenal Stakeholders.

- **Legal representatives.** May be an in-house corporate attorney or an outside law firm hired to represent the company if legal action is necessary.

Incident Response Plan

Preparation Phase

- Implement a "Defense in Depth" methodology.
- Keep employee updates for the new of the cyber security.
- Build Email Protections and Endpoint Protections.
- Doing regular backup with automate syncs via **cloud backup**.

Detection and Analysis

- Signs of an incident would be detect by email and endpoint protections, immediately in Security Team and IT Team for the potential cyber outbreak in different branch.
- User who detect suspicious changes to files, file names, or locations, or installation of unauthorized software, need to alert Secruity Team and IT Team via security hotline.

Containment Phase

- To integrated email and endpoint protection with network system to deploy into the branch so to isolate the infected devices automatical before other computer are targeted.

Eradication

- IT security and IT Team will be deploy to the brand island wide within 2 hours to reformat the entire affected computer.
- IT security and IT Team will also investigate the thoroughly with the user for the primary entry point and root cause.
- IT security and IT Team will also do patching vulnerabilities in the system.

Recovery

- The IT security and IT team would restoring impacted systems, data, and services to their pre-incident state
- ensure all systems have been hardened, patched, replaced, and tested

Lessons Learned

- IT security and IT team identify gaps in the organizational security practices. Was the lapse due to human error? Systems failure? Inadequate security practices?
- Identify the areas of improving for the incident response plan.
- Periodically test your Incident Response processes using activities like tabletop exercises.