**IT 211 – INFORMATION AND ASSURANCE SECURITY 1 LABORATORY NO. 1**

**Title: Information Assurance Case Study 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Course Yr/ Sec:** |  | **Date of Submission** |  |
| **Leader: Members:** | Tayao ,John Cristian  Villanueva, Bryan A.  Lazaro, Art Reignniel C.  Dela Rosa, Alwyn Troie T  Dela Cruz Jimp Murphy C. | | |
|  |  | | |

**Colonial pipeline in Ransomware Incidents**

**Introduction:**

The Colonial Oil Pipeline is the largest pipeline system for refined oil products in the U.S. originated in Houston, Texas that a ransomware attack occurred.

# Incident Analysis:

On May 07, 2021 at the evening, the Colonial oil pipeline in the United States was shutdown cause by the hackers infected the Colonial Pipeline IT Network by affecting many computer system, including the billing and accounting of the company. A large ransomware attack led the Colonial oil pipeline in the United States to shutdown, which led to panic buying and shortages. In the evening of 7 May 2021 after the attack, Colonial Pipeline informed the public about the shutdown of their 5500 mile-long pipeline transporting 45%45% of the US East Coast’s fuel supplies. This cause to gas shortages, panic buying, and rising fuel prices for the people in the Eastern US.

# Root Cause Analysis:

The root cause of the Colonial oil pipeline ransomware is that the attackers got into the Colonial oil pipeline network through an exposed password of an old VPN account. The company were low on cyber security that highlighted the vulnerabilities of the infrastructure in the United States.

# Information Assurance Practices:

After the cyberattack the Colonial oil pipeline forced the company to proactively close down operations and freeze IT systems after becoming the victim of a cyberattack. The operators now require multifactor authentication across all networks and filter network traffic by organizing operational technology assets into logical zones.

# Recommendations:

# One of the effective measures to improve information assurance is to update the account often also by having a high security protocols and system inspection will help to assure the security of the company data information. Latest system hardware can improve the security of the computer system to avoid data breaches, by enhancing the technical skills and knowledge of the company employee about the new computer technology or system. This proposed measures can greatly contribute in the data security.

# Implementation Plan:

# Step-by-step plan for implemented recommendations.

# *Conduct Security Assessment*

# Responsibility: IT Security Team

# Timelines: 1 month

# Resource requirements: Security assessment tools, IT expertise

# *Update Account Policies*

# Responsibility: IT Security Team

# Timelines: 2 weeks

# Resource requirements: Policy documentation, communication tools

# *Implement High Security Protocols*

# Responsibility: IT Security Team

# Timelines: 1 month

# Resource requirements: Implementation tools, communication tools

# *Schedule Regular System Inspections*

# Responsibility: IT Security Team

# Timelines: 1 month

# Resource requirements: Inspection tools, dedicated personnel

# *Upgrade System Hardware*

# Responsibility: IT Infrastructure Team

# Timelines: 3-5 months

# Resource requirements: Budget, hardware materials, IT personnel

# *Employee Training Programs*

# Responsibility: HR and IT Training Team

# Timelines: 1-2 months

# Resource requirements: Training materials, trainers

# Potential Challenges and Mitigation Strategies

# Resistance to change:

# Mitigation: Engage in clear and consistent communication about the benefits of security measures. Provide training and support to ease the transition.

# Budget constraints:

# Mitigation: Develop a comprehensive business case emphasizing the potential cost savings and risk reduction associated with implementing the proposed measures.

# User awareness and compliance:

# Mitigation: Regularly communicate the importance of security measures, conduct awareness campaigns, and provide ongoing training to reinforce best practices.

# Integration Issues:

# Mitigation: Pilot new measures in a controlled environment before full implementation. Address integration challenges incrementally and seek expert consultation if needed.

# Limited IT resources:

# Mitigation: Prioritize tasks based on risk and urgency. Consider outsourcing certain activities or leveraging automated tools to ease the workload.

# Lessons Learned:

Attackers can breach into unsecured internet connection, and also through low system security that’s why it is important to always check and update the systems for any anomalies. For the future incidents it is possible to breach in the current system or security due to the technology development that’s why the best practices in improving information assurance is by updating the system accounts and security.

# Conclusion:

# Information assurance is necessary even in the real world like personal documents that can be used by others if isn’t protected. In personal assets and organizational assets is very vulnerable in the internet world unlike in the real world because the internet is very wide and can access worldwide. Personal assets is a great target the hackers to be used from you to earn money that’s why protecting personal data must be protected to avoid any types of incidents.

*\*\*This case study activity aims to enhance Students' understanding of information assurance principles and their ability to apply them in real-world scenarios.*

**NPC confirms GCash incident caused by phishing attacks**

**Introduction**

The NPC confirm that some of several account has unauthorized caused by phising in Gcash. The unknown person who hack the several account Are the user of online gambling. NPC who investigate the incedent on may 9 the unauthorized perso have the personal data and many more. NPC and GIX have a meeting regarding about the phising attack to prevent other personal data of a person can be secured and the phising will be prevented.

**Introduction analysis**

The incident May 24, 2023, investigate by the NPCThat phising attack in several Gcash account.The investigation lead by NPC CID on may 9 where the personal data got hack. on may 19 GXI summited it's complains about the incident.

**Root cause analysis**

The the account attack is caused by phising who the unauthorized person will get the account personal information. Its a human error the unauthorized person took advantage of the gamblers account online gambling like "philwin" and "tapwin1".

**Information Assurance practice**

The effectiveness of an security system is to help the system of an company avoid attacks. To have a control of your system is important to your company to make sure your personal data will no leak in public. Make a training program about the attack and on how to avoid it.

**Recommendation**

I recommend that have a information about phising in gamblers and have a account user confirmation to the transaction. Prevent the unwanted sites that can cause you to click some link that can download viruses. Have an transaction history to make sure you can see the previous transaction you have.

**Implementation plan**

Create a system that can see the previous transaction of one person to another. Hire an cyber security that can monitor some of transaction and hire programmer that can create a system that can protect your company data. Some challenges are system maintenance and having trouble with some bugs of the system.

**Lessons learned**

Don't click to much unwanted links and website to prevent the phising attacks. Avoid suspicious activity and gambling online and others. The incident can be prevent with higher technology provided in the future.

**Conclusion**

The company that got attack can have a system security that can protect their personal data of company. Gcash acccounts got attack by an unauthorized person who atttacks the gamblers account. This conclusion follows a thorough investigation initiated by the NPC's CID, demonstrating their dedication to ensuring a safe and secure digital environment for all users. The importance of getting a security system is to protect your data from cyber attacks and threats.

**Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis**

**Introduction:**

# The importance of cybersecurity in the quickly changing digital economy of today cannot be emphasized. Effective detection and prediction systems become critical as insider threats become more common and pose a significant risk. This paper explores the state-of-the-art algorithms, research trends, and issues in insider threat detection and prediction. We provide important insights into these elements by addressing important topics through a systematic evaluation of 37 scientific articles published between 1950 and 2015. Our meta-analysis identifies and ranks the most promising algorithms, offering a thorough picture of the landscape from the prevalent usage of game theoretic approaches to the difficulties presented by unbounded patterns and collusion assaults.

# Root Cause Analysis:

The source code for Grand Theft Auto V was recently leaked due to a security breach that was the result of a threat actor organization that was targeting Rockstar Games. The hackers were able to obtain unauthorized access and steal company information, including the extremely private GTA 5 source code. In addition to jeopardizing Rockstar's confidential data, this hack has sparked serious questions about the security protocols used by the gaming sector.

# Information Assurance Practices:

Rockstar Games and other comparable organizations need to put strict assurance procedures in place in reaction to the GTA 5 source code leak in order to stop similar breaches in the future. Adopting cutting-edge cybersecurity techniques like intrusion detection, multi-factor authentication, and encryption is necessary for this. The protection against dangers like insider breaches and social engineering attempts is strengthened by regular security audits and employee training initiatives. Sensitive data exposure is restricted by access control and least privilege principles, and prompt identification and mitigation are made possible by ongoing monitoring and incident response procedures. Resilience is further improved by vendor risk management and secure software development methods. Stakeholder confidence and data protection are ensured by regulatory compliance. Together, these steps strengthen cybersecurity and reduce the possibility of further leaks.

# Recommendations:

A comprehensive strategy incorporating procedural, technical, and instructional improvements is advised as a reaction to information assurance vulnerabilities that have been found. First and foremost, technological precautions ought to be taken, such as putting strong encryption procedures in place to protect data, setting up intrusion detection systems for continuous monitoring, and utilizing endpoint protection programs to bolster device security. Enhancements to procedures comprise creating and implementing thorough security policies that control data processing and incident response.

# Implementation Plan:

# Start with a strong security policy that covers data protection, access limits, and permitted use. Inform staff members about cybersecurity threats and foster a culture of awareness. utilize the least privilege principle to restrict user access, and utilize sophisticated tools to keep an eye on their activities. Create and maintain incident response plans to quickly contain threats and promote open lines of communication for early identification. To fix vulnerabilities, use data encryption, Data Loss Prevention (DLP), and make sure your system is updated often. Establish effective exit procedures, work with HR to do comprehensive background checks, and carry out regular security assessments. This all-encompassing approach strengthens cybersecurity protection against any insider threats.

# Lessons Learned:

# Important takeaways from the effort to strengthen cybersecurity stress the need for a methodical approach. Important first measures include defining precise security guidelines, training staff, and restricting access. Early threat detection is made possible by rapid incident response, attentive monitoring, and open lines of communication. Vulnerability protections include encryption, data loss prevention, and frequent upgrades. Defenses are further strengthened by regular audits and cooperation with HR to implement strict hiring and leave procedures. Organizations may effectively manage and prevent insider threats by using these lessons as a basis.

# Conclusion:

# In conclusion, the case study emphasizes how crucial information assurance is to protecting organizational assets from hacks and data leaks. Through the implementation of proactive security measures, such as technical improvements, procedural modifications, and employee education programs, organizations can effectively reduce risks and strengthen their ability to fend off changing cyber threats. Maintaining the organization's long-term security and sustainability while staying ahead of new threats requires constant improvement in information assurance procedures.

**The need for effective information security awareness**

**In Password Attack**

**Introduction:**

# The study shows that in the Middle East, especially in the UAE, people aren't paying enough attention to being safe online. Even with advanced technology, not enough is done to teach people how to be secure, making the region an easy target for cyber threats. The research focuses on schools, universities, and organizations, looking at issues like Wi-Fi safety, falling for online scams, and using RFID technology securely. The timeline reveals problems dating back to before 2010, leading to in-depth studies uncovering weaknesses. It became urgent to start teaching people about online safety after 2010, as the region became more attractive to cybercriminals. Recommendations suggest creating effective programs to teach people about online safety, stressing the need for a complete approach to keeping information secure.

# Incident Analysis:

# In 2010, a big online problem happened in the Middle East, especially in the UAE. Before that, people weren't really careful online, making it easy for cybercriminals to target them. In 2010, studies found lots of unprotected Wi-Fi spots in Dubai and Sharjah, showing a problem with wireless security. At the same time, people were easily tricked by phishing attacks, risking their personal and banking info. Another study found that people didn't understand RFID technology well, which could lead to privacy issues. All these discoveries showed that there was an urgent need to teach people about online safety. The incident proved that cybercriminals really liked targeting the region, so recommendations were made for strong programs to teach people about keeping info safe online. The impact of the problem reached compromised data, systems, and network security, stressing the importance of a complete approach to protecting digital stuff.

# Root Cause Analysis:

# The problem in the Middle East in 2010 happened because of technical issues, mistakes by people, and problems with how things were done. A big survey found many Wi-Fi spots without protection, which cybercriminals used to cause trouble. People didn't know enough about online safety, making it easy for phishing attacks to work. There were also issues with how RFID technology was handled, putting users at risk. The incident showed bigger problems in the system, like not focusing enough on teaching people about online safety and being attractive to cybercriminals. Fixing these issues needs a complete plan, including improving tech defenses, teaching users better, and making strong rules for security. It also means dealing with broader problems in how the region gets ready for online threats to stop similar issues in the future.

# Information Assurance Practices:

# Checking how well things are kept safe online focused on important stuff: rules for safety, who can access what, keeping info secret, what to do if something bad happens, and teaching employees. The rules for safety were looked at to see if they were clear and followed, guiding users. Controls on who can access things were checked to make sure only the right people get in. Keeping info secret with encryption was checked to stop the wrong people from getting it. If something bad happened, the plan to deal with it was checked to be quick and clear. Teaching employees about staying safe online was also checked to be complete and done regularly. Overall, the check showed the need for clear rules, strong controls, good encryption, a clear plan for problems, and always teaching employees for a safe online space.

# Recommendations:

# To make sure information is safe, there are three main things to do. First, technically, we need to control who can access data and use strong encryption to keep it safe from the wrong people. Second, in terms of how we do things, we should regularly check and update our rules for safety to match new risks and make sure we can quickly respond if something goes wrong. Third, when it comes to educating people, we should quickly focus on improving how we keep data safe and what to do in case of a problem. In the medium term, we should update who can access what and teach people more. In the long term, we should always review and update our safety rules and keep teaching people to stay safe from new threats. This plan aims to fix immediate problems and set up a strong foundation for keeping information safe in the long run.

# Implementation Plan:

# To keep our information safe, we're doing three important things. Right away, we're making sure only the right people can access data and using strong encryption. We're also fixing how we respond if something goes wrong. In the next few months, we'll check and update who can access what and teach everyone more about staying safe online. In the long run, we'll always review and update our safety rules and keep teaching people about new online threats. This plan helps us solve problems now and build a strong foundation to keep our information safe for the future.

# Lessons Learned:

# The case teaches us that making sure people know how to stay safe online is super important. We need to regularly teach and remind everyone about it. Also, we should have a complete plan for safety, including technical stuff, how we do things, and educating people. It's vital to keep updating our rules for safety based on new risks, and if something goes wrong, we need a clear plan to deal with it. To avoid similar problems, we should be proactive by teaching people a lot, checking our technical systems regularly, and always trying to get better at keeping information safe. The case study tells us that information safety is always changing, so we need to keep learning and improving to make sure our online security stays strong and effective.

# Conclusion:

# The case study shows how important it is to keep our organizational stuff safe, especially in the Middle East, like in the UAE. It points out that people need to know more about staying safe online. The lessons tell us that we should have a complete plan for security, teach people a lot, regularly check our rules for safety, and quickly deal with any problems. This study reminds us that keeping our information safe isn't just about technology; it's a big strategy to protect data, systems, and networks from changing online risks.

**Destructive 'ILOVEYOU' computer virus strikes worldwide**

**Introduction:**

The topic is about "ILOVEYOU" virus rapidly spread through emails and chat programs, infecting computers across Asia, Europe, and the United States, causing significant disruptions. Major antivirus companies developed tools to combat the virus, which posed a severe threat to computer systems globally. The U.S. Senate experienced significant problems, leading to the shutdown of its internal email system, while the House of Representatives also grappled with its effects. This topic delves into the spread of the "ILOVEYOU" virus, the role of antivirus tools in halting its progression, and the response strategies adopted by government organizations to mitigate the threat posed by the malware.

# Incident Analysis:

The "ILOVEYOU" virus started in Hong Kong on May 4, 2000, and quickly spread worldwide by May 5, infecting computers in Asia, Europe, and the United States. Antivirus companies like Symantec and F-Secure made tools to fight the virus between May 5 and May 7. On May 8, 2000, the U.S. Senate's computer system got infected, so they shut down their email to stop it from spreading more. From May 8 to May 10, they worked hard to stop the virus, sending warnings and using antivirus measures. By May 11, 2000, the House of Representatives had fewer problems, but they found and removed lots of the virus from their systems. The virus risked harming data, systems using Microsoft Outlook, and network operations.

# Root Cause Analysis:

The "ILOVEYOU" issue happened because of computer problems, mistakes people made, and not having good plans. The virus took advantage of issues in Microsoft Outlook and chat programs, quickly spreading through emails and chats. People accidentally let the virus in by opening bad files or clicking on harmful links. This shows we need to teach people better about staying safe online. Also, not having good security plans and training for employees let the virus get into organizations easily. This incident tells us we should have strong rules, teach people well, and be ready to defend against new problems to keep our systems safe.

# Information Assurance Practices:

To make things better, we need a plan. First, we review and update security rules with the IT Security Team and Compliance Officer for one month, using tools and people to do it. Second, we make access controls stronger with the IT Operations Team and System Administrators for two months, giving them software and training. Third, we add encryption with the IT Security Team and Network Administrators for three months, getting software, hardware, and training. Lastly, we make incident response better with the Incident Response Team and IT Security Team, starting in two months and needing documents, training, and drills. Challenges like not wanting to change, not having enough resources, things being too hard, and following rules can be fixed with talking clearly, deciding what's most important, teaching and helping, and checking often to make sure we're following the rules.

# Recommendations:

To make things safer, follow these steps. First, update security rules to deal with new problems and make sure everyone knows what they should do. Second, control who can access our systems by giving different levels of access based on their jobs and checking regularly. Third, use encryption to protect our data when we send it and store it. Fourth, have clear plans for when something bad happens and practice them often. Invest in smart tools to find and stop threats and improve our procedures by making better plans and checking how we're doing regularly. Teach people how to stay safe and always keep an eye on things to be ready for new problems. It's important to focus on important upgrades, responding to incidents better, teaching employees, and keeping an eye on things all the time to stay safe from new threats.

# Implementation Plan:

# To improve safety, follow these steps: First, update security rules to handle new issues and ensure everyone knows their roles. Second, manage system access by giving different levels of access based on job roles and regularly checking permissions. Third, use encryption to protect data during transmission and storage. Fourth, create clear plans for emergencies and practice them regularly. Invest in tools to detect and stop threats, improve procedures by making better plans, and regularly check performance. Educate people on staying safe and stay vigilant for new problems. Focus on essential upgrades, better incident responses, employee training, and constant monitoring to stay safe from new threats.

# Lessons Learned:

The "ILOVEYOU" case shows us some important things. Email systems can get viruses like "ILOVEYOU", so we need strong email security. People's mistakes made the virus spread, so we must teach them about staying safe online. Acting fast when viruses come is important to protect our systems and data. To stop more incidents, we need to train people better, have stricter security rules, check for problems often, and use smart tools to find threats. It's important to always make our security better, teach people, and share what we know to stay safe from new problems.

# Conclusion:

The "ILOVEYOU" virus spread fast through emails and chats, hitting government and business computers worldwide. It shows how important it is to keep our systems safe. We need strong security rules, control who gets access, use encryption, and have plans for when things go wrong. This incident reminds us to always make our systems better to stay safe from new threats.

*\*\*This case study activity aims to enhance Students' understanding of information assurance principles and their ability to apply them in real-world scenarios.*