ONLY FOR REPEATING OR NON-REGULAR STUDENTS
INFORMATION SECURITY ASSIGNMENT
(COUNTED TOWARDS SESSIONAL MARKS)

Read the following 4 case studies and answer the questions given at the end of each case study. Submit the answers in a pdf file. Each student should submit the pdf file with the student name and CMS ID via email to faisal.khan@gatech.edu by Sunday September 18, 2022.

1.Hotel CEO Finds Unwelcome Guests in Email Account

SCENARIO:

The CEO of a boutique hotel realized their business had become the victim of wire fraud when the bookkeeper began to receive insufficient fund notifications for regularly recurring bills. A review of the accounting records exposed a serious problem. At some point a few weeks before, the CEO had clicked on a link in an email that they thought was from the IRS. It wasn't. When they clicked the link and entered their credentials, the cyber criminals captured the CEO's login information, giving them full access to intimate business and personal details.

ATTACK:

Social engineering, phishing attack.

A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with malware.

RESPONSE:

The hotel's cash reserves were depleted. The fraudulent transfers amounted to more than $1 million. The hotel also contacted a cybersecurity firm to help them mitigate the risk of a repeat attack.

IMPACT:

The business lost $1 million to an account in China. The funds were not recovered.

LESSONS LEARNED:

1. 1 Teach staff about the dangers of clicking on unsolicited email links and attachments, and the need to stay alert for warning signs of fraudulent emails. Engage in regular email security training.
2. 2 Implement stringent wire transfer protocols and include a secondary form of validation.
3. 3 Have a cyber incident response plan ready to implement!

QUESTIONS:

- **Knowing how the firm responded, what would you have done differently?**
- **What are some steps you think the firm could have taken to prevent this incident?**

2.A Construction Company Gets Hammered by A Keylogger

SCENARIO:

A small family-owned construction company made extensive use of online banking and automated clearing house (ACH) transfers. Employees logged in with both a company and user-specific ID and password. Two challenge questions had to be answered for transactions over $1,000.

The owner was notified that an ACH transfer of $10,000 was initiated by an unknown source. They contacted the bank and identified that in just one week cyber criminals had made six transfers from the company bank accounts, totaling $550,000. How? One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account.

ATTACK:

Cyber criminals were able to install malware onto the company's computers, using a keylogger to capture the banking credentials.

A keylogger is software that silently monitors computer keystrokes and sends the information to a cyber criminal. They can then access banking and other financial services online, using valid account numbers and passwords.

RESPONSE:

The bank was able to retrieve only $200,000 of the stolen money in the first weeks, leaving a loss of $350,000. The bank even drew over $220,000 on the business' line of credit to cover the fraudulent transfers. Not having a cybersecurity plan in place delayed the company response to the fraud.

The company also sought a cybersecurity forensics firm to:
• help them complete a full cybersecurity review of their systems • identify what the source of the incident was
• recommend upgrades to their security software

IMPACT:

The company shut down their bank account and pursued legal action to recover its losses. The business recovered the remaining $350,000 with interest. No money for time and legal fees was recovered.

LESSONS LEARNED:

1 Get notified - set up transaction alerts on all credit, debit cards and bank accounts.

2. 2 Restrict access to sensitive accounts to only those employees who need access; change passwords often.

3. 3 Companies should evaluate their risk and evaluate cyber liability insurance options.
4. 4 Choose banks that offer multiple layers of authentication to access accounts and transactions.
5. 5 Create, maintain, and practice a cyber incident response plan that is rapidly implementable.
6. 6 Cyber criminals deliver and install malicious software via email. Train employees on email security.

QUESTIONS:

- **Knowing how the firm responded, what would you have done differently?**
- **What are some steps you think the firm could have taken to prevent this incident?**

3.Stolen Hospital Laptop Causes Heartburn

SCENARIO:

A health care system executive left their work-issued laptop, which had access to over 40,000 medical records, in a locked car while running an errand. The car was broken into, and the laptop stolen.

ATTACK:

Physical theft of an unencrypted device.

Encryption is the process of scrambling readable text so it can only be read by the person who has the decryption key. It creates an added layer of security for sensitive information.

RESPONSE:

The employee immediately reported the theft to the police and to the health care system's IT department who disabled the laptop's remote access and began monitoring activity. The laptop was equipped with security tools and password protection. Data stored on the hard drive was not encrypted – this included sensitive, personal patient data. The hospital had to follow state laws as they pertain to a data breach. The U.S. Department of Health and Human Services was also notified. Personally Identifiable Information (PII) and Protected Health Information (PHI) data require rigorous reporting processes and standards.

After the theft and breach, the health care system began an extensive review of internal policies; they created a discipline procedure for employees who violate security standards. A thorough review of security measures with internal IT staff and ancillary IT vendors revealed vulnerabilities.

IMPACT:

The health care system spent over $200,000 in remediation, monitoring, and operational improvements. A data breach does impact a brand negatively and trust has to be rebuilt.

LESSONS LEARNED:

1. 1 Companies must establish and train employees on secure handling of work-issued devices.
2. 2 Devices must be safely stored when not in the immediate presence of the employee.
3. 3 Companies must take steps to encrypt data wherever it is stored or transmitted. Employees should have a clear understanding of the importance of encryption and how to use it.
4. 4 Companies must understand and know their responsibilities under the data breach notification laws of the state(s) in which they operate.
5. 5 A regular review of the company's security practices is imperative in modern organizations to prevent incidents, discover vulnerabilities, and to reduce impact of incidents.

QUESTIONS:

- **Knowing how the firm responded, what would you have done differently?**

- **What are some steps you think the firm could have taken to prevent this incident?**

4.A Dark Web of Issues for A Small Government Contractor

SCENARIO:

The CEO of a government contracting firm was notified that an auction on the dark web was selling access to their firm's business data, which included access to their military clients database. The CEO rapidly established the data being 'sold' was obsolete, and not tied to any government agency clients. How did this happen? The firm identified that a senior employee had downloaded a malicious email attachment, thinking it was from a trusted source.

ATTACK:

A phishing attack where malware is in the attachment of the email.

A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with a virus or malware

RESPONSE:

The company's IT management immediately shut off communications to the affected server and took the system offline to run cybersecurity scans of the network and identify any additional breaches. The firm's leadership hired a reputable cybersecurity forensics firm. Each potentially impacted government agency was notified. The U.S. Secret Service assisted in the forensics investigation.

IMPACT:

The operational and financial impact from the breach was extensive – costing more than $1 million: The company was offline for several days disrupting business; new security software licenses and a new server had to be set up.

LESSONS LEARNED:

1. 1 You are never too small to be a target. A cyber attack can happen to anyone.
2. 2 Teach staff about the dangers of clicking on unsolicited email links and attachments and emphasize the need to stay alert for warning signs of fraudulent emails.
3. 3 Install and regularly update anti-virus, network firewall, and information encryption tools to scan for and counteract viruses and harmful programs.
4. 4 Conduct ongoing vulnerability testing and risk assessments on computer networks.

QUESTIONS:

- **Knowing how the firm responded, what would you have done differently?**
- **What are some steps you think the firm could have taken to prevent this incident?**