Dublin Business School

CONTINUOUS ASSESSMENT TASK 1

Organisational and Societal Cybersecurity.

Module Leader: Darek Mizak

Submitted by: Nikant Sharma Msc in Cyber Security - 20005553

Table of Content

Task 1: Cybersecurity Risk Management for Fintech SaaS-Based Banking Application.

Overview

It is crucial to have a strong cybersecurity framework in the highly regulated financial industry, especially when creating and providing Software as a Service (SaaS) solutions to banking institutions. At the vanguard of innovation is our fintech company, which is entrusted with creating a mobile application and web portal that can be customised for small and medium-sized banks. Nonetheless, this role entails the obligation to comply with strict regulatory standards, particularly those stipulated by the Central Bank of Ireland. In addition to outlining the cybersecurity risks that are intrinsic to our business, especially with regard to third-party suppliers, this report will offer a thorough risk management procedure that will serve to both reduce these risks and reassure our clients of our dedication to the highest standards of information security.

Cybersecurity Risks' Nature

Our organisation's main cybersecurity threats are related to the sensitive and vital nature of the financial data we manage. We are tasked with protecting sensitive personal and financial data because we supply SaaS to banks. If this data is hacked, there might be serious financial losses, harm to our brand, and legal repercussions. The dangers encompass a range of potential outcomes, including but not restricted to: data breaches, unauthorised access to confidential information, Distributed Denial of Service (DDoS) attacks, and the possible exploitation of vulnerabilities in our application or underlying infrastructure. Because of the nature of the financial services sector, which places a high value on trust and dependability, even little cybersecurity errors can have far-reaching effects.

Hazards Associated with Third-Party Suppliers

There are more risks associated with our dependence on outside vendors for infrastructure, software, and security services. Despite being crucial to our operations, these suppliers may also serve as entry points for cyberattacks. For example, our platform may be indirectly compromised if the security measures of a third-party supplier are insufficient or if they suffer a breach. Furthermore, third-party programmes and services that interface with our application may contain security holes that bad actors could use to access our system. Our platform's intricate network of dependencies with outside vendors necessitates strict control and ongoing observation to guarantee that third-party risks are adequately handled.

Process for Risk Management Recommendation

I advise the establishment of an extensive risk management procedure built on the ISO/IEC 27001 framework in order to handle the risks stated above. This framework ensures that we can maintain the highest standards of security by offering a methodical approach to managing sensitive company information.

The following elements ought to be a part of the risk management process:

1. Risk Assessment and Identification: This stage entails locating possible risks, classifying them according to likelihood and impact, and recording them in a risk register. All facets of our business operations, such as the SaaS platform, internal procedures, and third-party integrations, should be evaluated.
2. Risk Mitigation Strategies: We need to create plans to lessen hazards as soon as they are recognised. This can entail putting in place more robust encryption techniques, improving access control systems, carrying out frequent security audits, and putting strict contractual arrangements in place to guarantee that outside suppliers abide by our security standards.
3. Constant Monitoring and Review: Maintaining cybersecurity requires ongoing attention rather than a one-time effort. By conducting routine system monitoring and reviewing our risk management procedures on a regular basis, we will be able to adjust to new risks and changing legal requirements. This includes ongoing vulnerability assessments, frequent penetration testing, and real-time monitoring for possible intrusions.
4. Incident Response Planning: We can never completely rule out the chance of a security breach, no matter how careful we are. As a result, having a clear incident response plan in place is essential. In the event of a security issue, this plan should specify what has to be done for immediate containment, investigation, and remediation. Furthermore, it is imperative to develop unambiguous communication mechanisms in order to swiftly and transparently notify impacted clients.

Application of the Risk Management Framework

Our organisation is especially well-suited to the ISO/IEC 27001 framework because of its emphasis on continuous development and all-encompassing approach to controlling information security threats. Through the implementation of this framework, we can guarantee that every facet of our security protocols is in line with global norms, thus fostering trust among our clientele and interested parties. Our risk management procedure will be heavily reliant on the elements of this framework, such as its continuous monitoring procedures, control objectives, and risk assessment methodology.

Risk Determination and Evaluation

I have determined and evaluated the following four major cybersecurity threats using the above-described methodology:

Data breach:A data breach is when someone gains illegal access to private financial information, which could result in theft or data breaches. Because of this risk's high possibility and impact, it is imperative that strong encryption and access control measures be put in place.

Service Disruption (DDoS Attack):Disruption of Services (DDoS assault): In the event of a DDoS assault, our clients may experience severe disruptions as our services become unavailable. The likelihood of this risk is moderate, but its impact is considerable, necessitating the purchase of sophisticated DDoS mitigation techniques and solutions.

Vendor Compromise by Third Parties: We could be compromised if there was a security breach at one of our third-party suppliers. Although there is some danger involved, it may be reduced by implementing stringent security measures and regularly auditing our vendors.

Exploitation of Vulnerabilities: Improper use of our program could result in service interruption or illegal access. The chance of this danger is considerable, but it is manageable with prompt patching and routine vulnerability checks.

Planning for Incident Response

Our top goals in the case of a data loss or security breach will be to promptly restore services and minimise any negative effects on our clients. As part of our incident response plan, we will follow pre-established protocols to locate and contain the breach, look into its underlying cause, and take appropriate action. In addition, we will be prepared with a communication strategy that will enable us to promptly and accurately inform impacted clients, upholding transparency and earning their confidence. We will continue to prioritise training our employees to react to situations quickly and efficiently in order to maintain readiness.

Practical Recommendations

To improve our cybersecurity posture, I suggest implementing the following doable steps:

Adopt Multi-Factor Authentication (MFA): To make unauthorised access considerably more difficult, implement MFA at all access points.

Regularly Provide Security Training Make certain that all staff members, even those employed by outside companies, receive frequent training on security best practices.

Apply Cutting-Edge Threat Detection Tools: Invest in technologies that instantly identify and neutralise such threats using AI and machine learning.

Put Vendor Management Policies in Writing: Formally manage third-party contractors by establishing standards for security, conducting frequent audits, and coordinating incident response.

These suggestions are made to make sure that our company not only complies with legal obligations but also exhibits leadership in cybersecurity management. They are made to be workable and in line with industry best practices.

ISO/IEC 27001

Following the ISO/IEC 27001 standard is not only legally required but also strategically crucial for our fintech company, which develops SaaS-based banking applications, in order to protect sensitive financial data and uphold client confidence. Given the nature of our operations, this globally recognised standard offers a complete framework for controlling and safeguarding information security, which is essential. The creation of thoroughly defined information security policies is one of the fundamental components of ISO/IEC 27001 standards. Our cybersecurity efforts are based on these principles, which provide precise recommendations for data protection, appropriate use of IT resources, and managing information security throughout the entire company. A strong data protection strategy, for example, is necessary to specify the encryption standards, access controls and data classification process that safeguard our client’s financial information.

An additional crucial element of ISO/IEC 27001 is asset management. To ensure accountability, we must assign ownership to each asset and keep a thorough inventory of everything from software and hardware to customer data. By appropriately classifying information according to its level of sensitivity, we can implement the right security controls and make sure that private data is handled with the highest care. Furthermore, the standard's focus on access control is crucial for our situation. The danger of unauthorised access is greatly decreased when role-based access control (RBAC) and multi-factor authentication (MFA) are implemented across all access points. This guarantees that only authorised users have access to important systems and data.

Even if the digital components of our platform may be our main focus, ISO/IEC 27001 emphasises the significance of environmental and physical security. Whether in data centres or cloud infrastructures, our SaaS platform depends on safe hosting environments that need to be shielded from external dangers. To guarantee the continuation of our services, this entails putting in place stringent access controls, surveillance, and environmental safeguards including fire suppression systems. Another crucial issue is communication security, especially for protecting data while it is in transit. Strong protocols like TLS must be used to encrypt all data transfers between our clients and the SaaS platform. To guard against outside threats, network security measures like intrusion detection systems and firewalls must also be in place.

Even if the digital components of our platform may be our main focus, ISO/IEC 27001 emphasises the significance of environmental and physical security. Whether in data centres or cloud infrastructures, our SaaS platform depends on safe hosting environments that need to be shielded from external dangers. To guarantee the continuation of our services, this entails putting in place stringent access controls, surveillance, and environmental safeguards including fire suppression systems. Another crucial issue is communication security, especially for protecting data while it is in transit. Strong protocols like TLS must be used to encrypt all data transfers between our clients and the SaaS platform. To guard against outside threats, network security measures like intrusion detection systems and firewalls must also be in place.

The standard's emphasis on compliance and business continuity is also very important. The implementation of a disaster recovery plan (DRP) and the completion of a business impact analysis (BIA) guarantee the prompt restoration of vital IT systems and data in the event of an interruption. To preserve our reputation with clients and regulatory agencies, we must consistently check and record adherence to legal and regulatory standards, such as the GDPR and particular financial legislation in Ireland. In order to guarantee that our information security management system (ISMS) adapts to new threats and is in line with organisational objectives, regular internal audits, management reviews, and corrective actions are encouraged by ISO/IEC 27001. We not only improve our security posture by incorporating these elements into our cybersecurity strategy but also reaffirm our dedication to upholding the strictest information security guidelines, protecting the faith that our clients have in us.

Task 2: Analysis of Significant Data Breach

Overview of the Incident

The MOVEit Transfer data breach, which was discovered in June 2023, was one of the biggest in the previous 12 months. The popular file transfer application MOVEit Transfer was compromised by the Clop ransomware organisation. A zero-day vulnerability in the program was exploited by the attackers to gain access to and steal confidential information from multiple organisations across the globe. Millions of records comprising financial and personal information were made public as a result of the hack, which had an impact on a wide range of industries including government agencies, financial services, and healthcare.

An SQL injection vulnerability was used in this incident to provide attackers access to the software's database and enable them to insert malicious SQL code. As a result, they were able to get around security measures and access private information that was kept on the MOVEit Transfer servers without authorisation. Using this access, the Clop ransomware group—which is well-known for its proficiency in taking advantage of these kinds of vulnerabilities—exfiltrated data and threatened to make it public unless a ransom was paid. The event brought to light serious flaws in the way businesses safeguard and maintain third-party software, especially when it comes to sensitive data.

Analysis of the Verizon Data Breach Investigations Report (DBIR)

Examining this incident under the prism of the Verizon Data Breach Investigations Report (DBIR) for 2023 reveals that the MOVEit Transfer breach is consistent with a number of the report's prevalent trends. According to the DBIR, there has been an increase in assaults that take use of online application vulnerabilities, especially those that involve ransomware. The paper also thoroughly documents the usage of SQL injection as an attack vector, suggesting that this kind of vulnerability is still a serious concern. The MOVEit breach is representative of a larger trend in which thieves exploit weaknesses in third-party software to obtain access to sensitive data, rather than being unique in the use of these techniques.

The MOVEit incident is unique, though, due to its scope and targeted nature. The targeted file transfer application is widely used and vital to many organisations' everyday operations. The incident shows how a single flaw in widely used software can have a domino effect on several industries, exposing a large amount of data and seriously disrupting business operations.

The type of threat and vulnerability that were exploited

Exploiting a zero-day SQL injection vulnerability was the main threat in the MOVEit Transfer hack. By inserting malicious SQL queries into an entry field and forcing them to run, attackers can obtain unauthorised access to the backend database using a technique known as SQL injection. In this instance, the attackers were able to get around authentication restrictions and access private information thanks to SQL injection. Because the vulnerability was a zero-day flaw—meaning that neither the software vendor nor the affected organisations knew about it at the time of the attack—it posed a particularly serious risk because it prevented them from applying patches or other mitigations before the breach happened.

Using this vulnerability, the Clop ransomware group—which has a history of focussing on similar flaws—conducted a massive data exfiltration operation. After they got the data, they used a standard technique used by ransomware: they demanded money in return for keeping the stolen data secret. The event emphasises how crucial it is to conduct routine security audits and promptly repair software vulnerabilities, especially in systems used to handle sensitive data.

Acquired Knowledge and Preventive Actions

Organisations can learn numerous important lessons from the MOVEit Transfer incident. It first emphasises how vital it is to thoroughly and continuously monitor third-party software. Strict vendor management procedures must be implemented by organisations, and this includes conducting routine security evaluations of the software they use, particularly for applications that handle sensitive data. The event also emphasises how critical it is to promptly manage vulnerabilities. Organisations must to take a proactive stance in spotting and fixing such security holes before hackers may take advantage of them.

The implementation of multi-layered security safeguards is important in order to avert similar disasters in the future. These ought to include frequent code reviews, vulnerability scanning to find and fix security flaws, and the deployment of web application firewalls (WAFs) to detect and block SQL injection attempts. Organisations should also spend money on sophisticated threat detection systems that can quickly address possible breaches and continuously scan the environment for unusual activities. Additionally, it is imperative to guarantee that staff members have the necessary training to identify and swiftly disclose any symptoms of a breach, since early identification can greatly lessen the damage of an attack.

Updates on Security Awareness Training

Enhancing our knowledge of vulnerabilities and fraudsters' strategies is essential if we are to improve our organization's security posture and stop similar incidents. The purpose of this security awareness update is to inform staff members about the dangers of using third-party software and the value of quick vulnerability management.

Salient Features of the Security Awareness Slide:

Overview of the Incident:Describe the attack of a zero-day SQL injection vulnerability in the MOVEit Transfer breach.

Learnings: Stress the value of timely patching, frequent security audits, and effective vendor management procedures.

Preventive measures: include promoting the use of sophisticated threat detection tools, web application firewalls, and ongoing third-party software monitoring.

An overview of security awareness education

By taking use of a zero-day SQL injection vulnerability, a ransomware group exploited the MOVEit Transfer program in June 2023. Sensitive information belonging to many different types of organisations was made public by this occurrence. The hack highlights how important it is for businesses to handle third-party software security proactively and to fix vulnerabilities as soon as they can be used against them. Implementing multi-layered security controls, such as web application firewalls, advanced threat detection technologies, and constant monitoring, is essential to averting events of this nature. By implementing these safeguards, we can guarantee the security of our sensitive data and defend our company from similar attacks.

Task 3: Understanding and Mitigating Social Engineering Attacks

A Social Engineering Attack: What Is It?

Social engineering attacks are a kind of cyberthreat in which perpetrators use deception to trick victims into disclosing private information or taking activities that jeopardise an organization's security. In contrast to conventional hacking methods that depend on taking advantage of technological flaws, social engineering plays on people's fears, curiosity, trust, or ignorance. Phishing emails, pretexting, baiting, and tailgating are just a few of the various ways these assaults can trick people into unintentionally giving up access to private data or systems.

Social engineering's basic goal is to deceive people into evading standard security procedures. To win over the victim's trust, attackers could pose as reputable individuals like a service provider, coworker, or corporate boss. Once trust has been created, the victim may be fooled into clicking on dangerous links or downloading infected attachments, or they may be forced to give passwords, bank account details, or other private information. Successful social engineering assaults can have disastrous results, including financial losses, data breaches, and serious harm to the victimised organization's reputation.

Methods and Strategies Applied in Social Engineering Assaults

Although the techniques used in social engineering attacks vary, they frequently employ similar strategies meant to take advantage of human emotions and behaviour. Three methods that threat actors frequently employ are as follows:

Phishing: One of the most common types of social engineering is probably phishing. Usually, it entails sending phoney emails that seem to be from reliable sources, such banks, internet companies, or even other members of the victim's company. These emails frequently contain urgent messages that urge the receiver to open an attachment or click on a link, which can expose personal data or cause malware to be installed. A phishing email might, for instance, state that the recipient's account has been compromised and that they must reset their password right away. It would then take them to a phoney website that is intended to collect login information.

Pretexting: In order to deceive the victim into divulging information or carrying out a certain action, the attacker fabricates a scenario, or pretext. This might be phoning in as a government official demanding private information for a "regular audit" or assuming the identity of an IT support technician calling to "check" the user's login credentials. The ability of the attacker to fabricate a plausible tale and persuade the victim that their acts are required and justified is crucial to the effectiveness of pretexting.

Baiting: is the practice of taking advantage of people's curiosity or avarice by presenting an alluring offer, such as free software, a purported reward, or even a USB drive left in a public area. By accepting the bait, the victim unintentionally installs malware on their computer or gives the attacker access to it, for example, by plugging the USB drive into their computer or installing the "free" programme. Baiting capitalises on people's innate curiosity and inclination to investigate or seize seemingly innocuous situations.

Techniques to Reduce the Likelihood of a Successful Attack

Organisations need to take a multifaceted approach that incorporates employee education and technical defences to reduce the risk of social engineering attacks. Here are three crucial tactics to remember:

1. Employee Education and Awareness: A knowledgeable staff is the first line of defence against social engineering. Employees should have regular security awareness training to learn about the different kinds of social engineering attacks, how to spot them, and what to do if they see questionable activity. Simulated phishing exercises should be a part of training programmes in order to assess and validate staff members' abilities to recognise and react to any threats. Establishing a security-conscious culture can help organisations drastically lower the risk that workers will become victims of social engineering schemes.
2. Establishing strong Access Controls: In order to restrict the quantity of information that employees can access in accordance with their roles and responsibilities, organisations should implement strong access controls. The principle of least privilege guarantees that, even in the event that an attacker is successful in tricking an employee, the possible harm is reduced since the employee is not granted undue access to confidential information or vital systems. In order to provide an additional degree of protection and make it more difficult for attackers to achieve unauthorised access, even in the event that they manage to obtain legitimate login credentials, multi-factor authentication, or MFA, should also be installed.
3. Mechanisms for Incident Response and Reporting: Companies should set up explicit incident response procedures that let staff members report such social engineering attempts promptly and effectively. Defined points of contact for reporting events and processes for looking into and handling such reports should be part of these standards. A minor incident can be kept from growing into a big breach by reporting it promptly and taking immediate action. In addition, following a social engineering attempt, a comprehensive assessment needs to be carried out in order to pinpoint any vulnerabilities in the organization's defences and modify security protocols and training materials appropriately.

To conclude, social engineering assaults pose a serious risk to organisations since they prey on people rather than technical flaws in security. Organisations may significantly lower their risk of becoming victims of these kinds of assaults by being aware of the strategies employed by attackers and putting in place thorough training, strict access controls, and reliable incident response procedures. Keeping an alert and knowledgeable staff is the best line of defence against the persistent threat of social engineering.

Cybersecurity Awareness Presentation for Students Aged 14-16

Overview

Growing dependence on digital technologies makes some demographics—young people in particular—more susceptible to cybercrime. Our talk, which is intended for kids in grades 14 through 16, will cover potential cybersecurity risks and offer helpful tips on staying safe online. The talk will be brief and concentrate on the main risks that affect this age range, namely social engineering, phishing, and online privacy. Giving kids the skills and information they need to successfully navigate the digital environment is the aim.

Slide 1: Understanding Cybersecurity

Title: What is Cybersecurity?

Slide 2: Common Cyber Threats

Title: Common Cyber Threats You Should Know About

Slide 3: How to Stay Safe Online

Title: How to Protect Yourself Online

Slide 4: What To Do If Something Goes Wrong

Title: What To Do If You’re a Victim of Cybercrime

References

1. GDPR.eu (n.d.) *EU General Data Protection Regulation (GDPR)*. Available at: https://gdpr.eu/ (Accessed: 14 August 2024).
2. NIST (n.d.) *NIST Cybersecurity Framework*. Available at: https://www.nist.gov/cyberframework (Accessed: 14 August 2024).
3. Verizon (2023) *Data Breach Investigations Report (DBIR) 2023*. Available at: https://www.verizon.com/about/news/2024-data-breach-investigations-report-emea (Accessed: 14 August 2024).
4. OWASP (n.d.) *SQL Injection Overview*. Available at: https://owasp.org/www-community/attacks/SQL_Injection (Accessed: 14 August 2024).
5. Norton (n.d.) *Social Engineering - What It Is & How to Prevent It*. Available at: https://us.norton.com/blog/emerging-threats/what-is-social-engineering (Accessed: 14 August 2024).