浙江大學

《Big Data Security and Privacy Protection》

Project

题　　目：	Project
上课时间：	August 24th
授课教师：	Rongxing Lu
姓　　名：	杜宗泽
学　　号：	3220105581
组　　别：	个人
日　　期：	8月24日

Report on Cybersecurity Events and Guidelines for Securing Financial Big Data in Banks and Financial Institutions

1 Abstract

The recent cybersecurity events involving the bank hack and the potential exposure of personal data of 90,000 Canadians highlight the critical need for robust security measures in banks and financial institutions. This report aims to analyze the possible reasons behind these cybersecurity events and propose a comprehensive guideline for securing financial Big Data, including user data in banks and financial institutions. The guideline will include encryption methods and other security measures to ensure the protection of sensitive information.

2 Analysis of Cybersecurity Events:

2.1 Exploitation of Weaknesses in Security Systems

The hackers in the bank hack incident were able to gain access to personal information by exploiting weaknesses in the banks' security systems. Here are some of the weaknesses mentioned:

1. **Insufficient password validation**: The hackers claim that the banks were not checking if a password was valid until the security questions were input correctly. This allowed them to gain partial access to accounts by posing as authentic account holders who had forgotten their password.

2. **Insufficient authentication and vulnerability authorization mechanisms**: The hackers were able to reset the backup security questions and answers, which gave them access to the accounts. It seems that the banks were not adequately verifying the authenticity of the account holders during this process.

3. **Exploiting a mathematical algorithm**: The hackers used a common mathematical algorithm designed to quickly validate relatively short numeric sequences, such as credit card numbers and social insurance numbers. They claim that this algorithm helped them obtain account numbers, which further facilitated their access to the accounts.

2.2 Internal human factors of Hack

1. **Lack of Regular Security Audits and Penetration Testing:** The fact that the hackers were able to access sensitive information undetected indicates a potential lack of regular security audits and penetration testing. Financial institutions should conduct comprehensive security audits and penetration tests to identify vulnerabilities and address them proactively.

2. **Inadequate Employee Training and Awareness:** Human error can often lead to security breaches. It is crucial for banks and financial institutions to provide regular training and awareness programs to employees regarding cybersecurity best practices, such as recognizing phishing attempts, using strong passwords, and reporting suspicious activities promptly.

The above things only pointed out the main potential influencing factors of this security attack, but it inadvertently penetrates into our life and potentially threats us. Therefore, in the next chapter, I provide guidance for reference based on some of the content we have learned in class and the knowledge from Internet.

3 Guidelines for Securing Financial Big Data

3.1 Building a strong security foundation

3.1.1 Establishing a comprehensive security framework:

Financial institutions should establish a comprehensive security framework that encompasses policies, procedures, and controls to protect their Big Data assets. This framework should align with industry standards and best practices, such as ISO 27001 or NIST Cybersecurity Framework. It should include elements such as risk management, incident response, access control, and data protection.

1. **Risk management:**
   Conduct regular risk assessments to identify potential vulnerabilities and threats to financial Big Data. This involves evaluating the likelihood and impact of risks and prioritizing mitigation efforts accordingly. Implement a risk management framework that includes risk identification, assessment, mitigation, and monitoring.

2. **Incident response:**
   Develop a robust incident response plan that outlines the steps to be taken in the event of a security incident. This plan should include procedures for detecting, containing, eradicating, and recovering from security breaches. Regularly test and update the plan to ensure its effectiveness.

3. **Access control:**
   Implement strong access control mechanisms to ensure that only authorized individuals can access financial Big Data. This includes employing role-based access control (RBAC), where access privileges are assigned based on job roles and responsibilities. Implement least privilege principles to restrict access to the minimum necessary level required to perform job functions.

3.1.2 Conducting risk assessments and threat modeling:

Financial institutions should regularly conduct risk assessments and threat modeling exercises to identify potential vulnerabilities and threats to their Big Data assets. This involves analyzing the organization's infrastructure, systems, and processes to identify weaknesses and potential attack vectors.

1. **Risk assessments:**
   Conduct regular risk assessments to identify and prioritize risks to financial Big Data. This involves evaluating the likelihood and impact of risks, considering factors such as data sensitivity, regulatory requirements, and business impact. Use risk assessment methodologies such as qualitative or quantitative risk analysis to quantify and prioritize risks.

2. **Threat modeling:**
   Perform threat modeling exercises to identify potential threats and attack vectors that could compromise financial Big Data. This involves analyzing the system architecture, identifying potential vulnerabilities, and assessing the likelihood and impact of different threats. Use threat modeling frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) or DREAD (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) to guide the process.

3.1.3 Implementing a robust security governance structure:

Financial institutions should establish a robust security governance structure to ensure that security policies and controls are effectively implemented and monitored.

1. **Security policies and procedures:**
   Develop and enforce security policies and procedures that address the specific risks and requirements of financial Big Data. These policies should cover areas such as data classification, access control, encryption, incident response, and employee awareness. Regularly review and update these policies to reflect changes in the threat landscape and regulatory requirements.

2. **Security awareness and training:**
   Provide regular security awareness and training programs to educate employees about their roles and responsibilities in protecting financial Big Data. This includes training on topics such as phishing awareness, password hygiene, social engineering, and secure coding practices. Foster a culture of security awareness and encourage employees to report any suspicious activities.

3. **Security audits and assessments:**
   Conduct regular security audits and assessments to evaluate the effectiveness of security controls and identify areas for improvement. This includes internal audits, external assessments, and penetration testing. Use the results of these audits to drive continuous improvement and address any identified vulnerabilities or weaknesses.

4. **Security metrics and reporting:**
   Establish security metrics and reporting mechanisms to monitor the effectiveness of security controls and track key security indicators. This includes metrics such as the number of security incidents, response times, and compliance with security policies. Regularly review and analyze these metrics to identify trends, measure progress, and make informed decisions.

The above measures provide a solid basis for implementing specific security controls and practices to safeguard financial Big Data. And Meanwhile, we should raise the human security awareness not only the staff member but also the customers so that we could significantly avoid the human factors.

3.2 Application of security

3.2.1 Secure software development lifecycle (SDLC) practices:

Financial institutions should adopt secure software development practices throughout the entire software development lifecycle to ensure that applications handling financial Big Data are built with security in mind.

1. **Requirements gathering and threat modeling:**
   During the requirements gathering phase, identify potential security requirements and conduct threat modeling exercises to identify potential vulnerabilities and threats. This helps in designing and implementing appropriate security controls from the early stages of development.

   Threat modeling involves identifying potential threats, assessing their impact, and determining the likelihood of occurrence. By understanding the potential risks, developers can prioritize security measures and allocate resources accordingly. This process helps in identifying potential vulnerabilities and designing countermeasures to mitigate them.

2. **Secure coding practices:**
   Promote secure coding practices among developers, such as input validation, output encoding, and proper error handling. Emphasize the use of secure coding frameworks and libraries to prevent common vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Regularly train developers on secure coding practices and provide them with up-to-date resources and guidelines.

   Secure coding practices involve writing code that is resilient to attacks and follows established security guidelines. This includes validating user input, sanitizing data, and using parameterized queries to prevent SQL injection attacks. By adhering to secure coding practices, developers can reduce the risk of introducing vulnerabilities into the application code.

3. **Code reviews and static analysis:**
   Conduct regular code reviews to identify security vulnerabilities and coding errors. Use automated static analysis tools to scan the codebase for potential security flaws. Address identified issues promptly and ensure that secure coding practices are followed consistently.

   Code reviews involve a thorough examination of the application code to identify security vulnerabilities, logic errors, and coding mistakes. This process helps in identifying potential weaknesses and provides an opportunity to fix them before the application is deployed. Automated static analysis tools can assist in identifying common coding errors and vulnerabilities, such as buffer overflows or insecure cryptographic implementations.

4. **Secure third-party components:**
   Assess the security of third-party components and libraries used in applications. Regularly update these components to ensure that any known vulnerabilities are patched. Maintain an inventory of all third-party components and monitor security advisories to stay informed about any security updates or patches.

   Third-party components and libraries can introduce vulnerabilities into an application if they are not properly maintained or if they contain known security flaws. It is important to assess the security of these components before integrating them into the application and to keep them up to date with the latest security patches.

3.2.2 Regular vulnerability assessments and penetration testing:

Financial institutions should conduct regular vulnerability assessments and penetration testing to identify and address vulnerabilities in their applications handling financial Big Data.

1. **Vulnerability assessments:**
   Perform regular vulnerability assessments to identify potential weaknesses in applications. Use automated vulnerability scanning tools to scan applications for common vulnerabilities such as insecure configurations, outdated software versions, and weak authentication mechanisms. Address identified vulnerabilities promptly and prioritize them based on their severity.

   Vulnerability assessments involve scanning the application and its underlying infrastructure for known vulnerabilities. Automated vulnerability scanning tools can help identify common vulnerabilities and misconfigurations. By regularly conducting vulnerability assessments, financial institutions can identify and address potential weaknesses before they are exploited by attackers.

2. **Penetration testing:**
   Conduct periodic penetration testing to simulate real-world attacks and identify vulnerabilities that may not be detected by automated tools. Engage professional penetration testers who have expertise in financial application security. Penetration testing should cover various attack vectors, including network, application,

and social engineering. Address identified vulnerabilities and weaknesses based on the findings of the penetration test.

Penetration testing involves simulating real-world attacks to identify vulnerabilities and weaknesses in the application. Professional penetration testers use a combination of automated tools and manual techniques to identify potential entry points and exploit vulnerabilities. By conducting regular penetration tests, financial institutions can identify and address vulnerabilities that may not be detected by automated tools.

3.3 Web application firewalls (WAF) and runtime application self-protection (RASP):

Financial institutions should consider implementing web application firewalls (WAF) and runtime application self-protection (RASP) mechanisms to enhance the security of their web applications handling financial Big Data.

1. **Web application firewalls (WAF):**
   Deploy WAF solutions to protect web applications from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). WAFs analyze incoming traffic and apply security rules to block or mitigate potential attacks. Regularly update WAF rules to stay protected against emerging threats.

   Web application firewalls act as a protective layer between the application and the external network. They inspect incoming traffic and apply security rules to block or mitigate potential attacks. WAFs can detect and block common attack patterns, such as SQL injection or XSS, before they reach the application.

2. **Runtime application self-protection (RASP):**
   Implement RASP solutions that provide real-time monitoring and protection for applications. RASP solutions integrate with the application runtime environment and can detect and respond to attacks in real-time. They can provide capabilities such as input validation, output encoding, and behavior monitoring. Regularly update RASP solutions to ensure they are equipped to handle new attack vectors.

   Runtime application self-protection solutions monitor the application's behavior during runtime and can detect and respond to attacks in real-time. RASP solutions can provide capabilities such as input validation, output encoding, and behavior monitoring to protect against common attack vectors. By implementing RASP solutions, financial institutions can enhance the security of their applications and respond to attacks in real-time.

3. **Secure configuration and hardening:**
   Ensure that web application servers and frameworks are securely configured and hardened. Disable unnecessary services, apply security patches and updates, and follow industry best practices for secure configuration. Regularly review and update the configuration to address any new vulnerabilities or emerging threats.

   Secure configuration and hardening involve applying security best practices to web application servers and frameworks. This includes disabling unnecessary services, applying security patches and updates, and following industry guidelines for secure configuration. Regularly reviewing and updating the configuration helps in addressing any new vulnerabilities or emerging threats.

Implementing secure software development practices, conducting regular vulnerability assessments and penetration testing, and leveraging web application firewalls (WAF) and runtime application self-protection (RASP) mechanisms, financial institutions can enhance the security of their applications handling financial Big Data.

4 Conclusion

Overall, the recent cybersecurity events in the banking sector highlight the need for banks and financial institutions to prioritize the security of financial big data, including user data. By implementing strong authentication measures, enhancing password management practices, conducting regular security audits, deploying intrusion detection and prevention systems, implementing encryption and data protection mechanisms, providing employee training and awareness, and developing an incident response and recovery plan, banks can significantly enhance their cybersecurity posture.

Collaboration and information sharing within the industry are also crucial for staying ahead of evolving threats. It is essential to continuously evaluate and update security measures to stay ahead of evolving cybersecurity threats and protect sensitive information effectively. By following these guidelines, banks can better secure financial big data and protect the privacy of their customers.