Business Case: A Scenario-based cybersecurity risk assessment for the Atlantic Canada Regional Bank

By Marc-André Léger, PhD

This business case was created to be used in my cybersecurity classes. It is used by students to learn how to perform cybersecurity risk assessments using a scenario-based approach, as presented in class. The case described here is about a fictitious small regional bank situated in Atlantic Canada. This bank was the victim of a cyber-attack in 2022. Following this important incident, a cybersecurity risk assessment analyst is mandated to perform a scenario-based cybersecurity risk assessment to help determine a cybersecurity action plan for 2024-2027. In the proposed exercise, students play the role of a full-time bank employee, working in the newly created cybersecurity group. This group is managed by the chief information security officer (CISO), reporting directly to the CEO and Board of directors.

Students and instructors can use this business case in a multitude of ways, depending on the objectives of your cybersecurity course. Here are some suggestions:

1. **Case Study Analysis:** Encourage students to critically analyze the business case. This will help them understand real-world challenges, the importance of rapid response, and the complexities involved in managing cybersecurity incidents.
2. **Scenario-Based Cybersecurity Risk Assessment:** Using the business case as a foundation, students can perform risk assessments to identify potential vulnerabilities, evaluate the associated risks, and propose mitigation strategies.
3. **Policy and Procedure Development:** Ask students to draft policies or procedures for ACRB to prevent future attacks. This could range from developing an incident response plan to creating a comprehensive cybersecurity policy.
4. **Ethical and Legal Aspects:** Discuss the ethical implications of the cyberattack, the bank's response, and the responsibilities of organizations. Additionally, delve

into the legal aspects, including compliance with regulations, potential lawsuits, and reporting requirements.

5. **Group Projects:** Divide the class into groups and assign each a particular aspect of the case (e.g., technical analysis, communication strategy, policy development). This promotes teamwork and ensures a comprehensive examination of the case.
6. **Reflection:** After all exercises, ask students to reflect on what they've learned, the importance of cybersecurity in today's digital age, and how they can apply these learnings in real-world roles.

Incorporating real or simulated business cases, like that of ACRB, into coursework provides students with practical experience, bridging the gap between theoretical learning and real-world application. By working through this case, students will not only grasp the complexities of cybersecurity but also hone their analytical and decision-making skills.

Introduction

Atlantic Canada Regional Bank (ACRB) is a small, community-centric bank in Atlantic Canada, supporting local businesses and households with financial needs. It was founded in 1952 in Halifax (Nova Scotia) by Charles-Xavier Gardiner. ACRB has a focus on providing personalized service and is committed to investing in the communities it serves. They provide a wide range of products and services, from personal savings accounts to small business loans. Their experienced staff is available to assist customers with their financial needs and goals. As part of its digital transformation started in 1990, ACRB has embraced technology to improve its services. Increasingly, ACRB has invested in IT infrastructure and customer service solutions. Since 2010, it has integrated digital banking products and services. More recently, they have also implemented AI-driven data analytics and marketing automation tools to help the bank better understand customer needs and optimize its customer experience.

All of this has exposed the bank to new risks. ACRB needs to ensure that its technology is protected, that customer data is safeguarded, and regulatory compliance requirements are respected. The bank must ensure that its systems are secure, and that the data collected is used responsibly. Finally, ACRB must ensure that its technology is always up-to-date and that its employees are properly trained on how to use the new systems. The 2022 cyber-attack underscored ACRB's cybersecurity vulnerabilities.

Atlantic Canada Regional Bank Branch Network

ACRB operates a total of 30 local branches spread across the Atlantic Canada region. Most branches are in small-town throughout the region, with an average of 12 employees, including the management staff. The total client-facing staff totals 500 individuals, from a total workforce of approximately 750, including the IT Teams (83) and newly created cybersecurity teams (20) discussed in this case.

In the smaller rural communities, it is the only bank with a local branch. There are a few larger branches as well. These branches are strategically located in the major cities of the Atlantic provinces, ensuring that the bank maintains a prominent presence in the region, as listed below:

- **Halifax, Nova Scotia:** This branch serves as the bank's headquarters and is situated in the heart of Halifax's business district. Due to its central location, it is one of the busiest branches and houses the executive offices.
- **St. John's, Newfoundland and Labrador:** Located in downtown St. John's, this branch manages the bank's operations for the Newfoundland and Labrador region.
- **Moncton, New Brunswick:** This branch in Moncton serves as the primary banking hub for New Brunswick and offers both personal and commercial banking services.

- **Charlottetown, Prince Edward Island:** Positioned centrally in Charlottetown, this branch is essential for catering to the banking needs of Prince Edward Island residents.

IT department of the Atlantic Canada Regional Bank

Since 1990, the IT department has grown. While investments where modest at first, this increased significantly in 2010. With the COVID crisis, the importance of IT as a strategic tool became even more evident. In the year prior to the incident described in this case, the total IT budget was CAD$ 50 million, including salaries, with a 5% increase planned for next year. Following the incident, the Board has authorized a CAD$ 10 million, non-recurrent budget, to deal with the crisis and implement new measures. It also allocated a recurring CAD$ 5 million for the newly created cybersecurity group, which will be reviewed based on the results and recommendations from the cybersecurity risk assessment being performed.

IT Infrastructure:

- **Core Banking System:** ACRB utilizes a proprietary core banking system, which manages everyday banking functions such as opening new accounts, processing transactions, loans, mortgages, and deposits. This system is integral to the bank's day-to-day operations and serves as its backbone. It was initially created in the early 70's and has been continuously updated since.
- **Data Centers:** ACRB operates two data centers, one primary center near its head office in Halifax (Nova Scotia) and one disaster recovery site located geographically apart in Moncton (New Brunswick). These data centers host bank critical servers, storage systems, and networking equipment, using equipment from various reputable hardware manufacturers.
- **Network Architecture:** A multi-layered network infrastructure supports ACRB, incorporating firewalls, switches, routers, and intrusion detection/prevention systems. The bank employs virtual and physical servers and uses VLANs to

segregate traffic types and user groups. Since 1998, all networking equipment purchased and implemented has been Cisco.

- **Cloud Integration:** While much of ACRB's infrastructure is on-premises, they have begun integrating certain non-critical applications and storage solutions with cloud providers to ensure scalability and flexibility. They use both Amazon AWS and Microsoft Azure.
- **Branch Connectivity:** Each branch of ACRB connects to the central infrastructure via secured VPN tunnels, ensuring encrypted communication and data integrity. Branches employ local servers for immediate needs but rely on the main data center for significant processing and data retrieval.
- **Customer Interfaces:** ACRB provides various digital platforms:
- **Online Banking Portal:** A secure web platform allowing customers to perform transactions, check balances, and manage their accounts.
- **Mobile Banking App:** A custom mobile application available on all major platforms (iOS, Android) offering most of the online banking portal's capabilities.
- **ATMs:** Networked machines are located throughout the region, allowing cash withdrawals, deposits, and account inquiries. Including ATMs installed in convenience stores and malls, the bank operates 800 ATM terminals.
- **Point of sale (POS) terminals:** ACRB offers a POS network for merchants. There are currently 700 terminals in use.
- **Security Infrastructure:** Given the sensitive nature of its operations, ACRB has invested in robust security solutions.
- **Firewalls and IDS/IPS:** Protecting network perimeters and monitoring suspicious activities.
- **Endpoint Security:** Solutions deployed on every workstation and server to protect against malware, ransomware, and other threats.
- **Multi-Factor Authentication (MFA):** For employees and customers accessing digital banking platforms.

- **Data Encryption:** Both in transit (over the network) and at rest (stored on servers).
- **Backup and Recovery:** ACRB has a structured backup and recovery solution, with daily backups stored both on-site for quick recovery and off-site for disaster recovery purposes.
- **Collaboration Tools:** To support its staff, ACRB employs various collaboration tools such as Microsoft Exchange email servers, Microsoft Office (Teams, SharePoint, and the Office business suite), Cisco Voice over IP (VoIP) solutions, Cisco video conferencing systems, and internal chat platforms.
- **Customer Support Systems:** ACRB utilizes a Customer Relationship Management (CRM) system from SAP to track customer interactions and support tickets. They also have an Interactive Voice Response (IVR) system for their call center. Apart from the core banking systems mentioned previously, SAP is used in all internal financial systems.

IT Team of the Atlantic Canada Regional Bank

ACRB boasts a robust Information Technology (IT) team of 83 full-time staff led by the Chief Information Officer (CIO), Michael L. Ross. The CIO's primary role is to set the bank's IT strategy. This involves overseeing technology operations. It ensures that the IT vision aligns seamlessly with the bank's overarching business goals. The current total IT staffing budget is CAD$ 9,5 million per year, including benefits.

The Infrastructure Team comprises 15 dedicated professionals. This includes Network Engineers who oversee the bank's networking infrastructure, from routers and switches to firewalls and VPNs. Working alongside them are System Administrators who oversee server health, software updates, and other critical system functions. Ensuring the integrity, performance, and security of the bank's databases are Database Administrators, a crucial trio within the team.

When it comes to safeguarding the bank's digital realm, the Cybersecurity Team steps up to the plate. This 10-person squad consists of Security Analysts who vigilantly monitor for potential threats and vulnerabilities. Incident Responders are always on their toes, ready to act when a security breach occurs. In addition, a duo of Security Architects constantly devises innovative strategies to enhance bank defense systems. This team is now being put outside of IT and will form the basis of the newly created cybersecurity group.

On the application side of things, the Application Development and Maintenance Team has 20 individuals. Software Developers work tirelessly to craft internal tools and external applications, like the online banking portal and mobile app. Complementing their efforts are QA Engineers, whose primary mission is to guarantee software solutions' reliability and robustness.

Ensuring smooth day-to-day operations, the End-User Support Team of 12 provides invaluable assistance to bank employees. Helpdesk Technicians offer the first line of IT support, handling common inquiries and challenges. For more intricate, hands-on IT concerns, Desktop Support Engineers are ready to intervene.

Since 2020, the CIO has stated that the banks future is undeniably in the clouds. ACRB's five-member Cloud and Integration Specialist team (5) knows this best. Cloud Engineers manage and optimize cloud-based services, while Integration Specialists ensure flawless connectivity between various IT systems and third-party tools.

Business Intelligence and Data Analytics, with its ten specialists (10), mine data daily for the bank. Data Scientists dive deep into data reservoirs to derive invaluable insights that aid bank decision-making. BI Analysts, using state-of-the-art data visualization tools, provide actionable reports to bank top brass.

Every successful IT project owes its success to meticulous planning and management. This is where the eight-strong team (8) of IT Project Managers and IT Business Analysts

comes in. Project Managers shepherd IT projects from inception to conclusion, while Business Analysts act as the linchpin between IT initiatives and bank business requirements.

Last but certainly not least, the Training and Development wing, with three (3) IT Training Specialists, ensures that the bank's IT team and staff remain abreast of the latest technological innovations, tools, and best practices.

The newly created cybersecurity group.

Following the cyber-attack in 2022, ACRB realized the dire need to enhance its cybersecurity infrastructure. Responding to this pressing requirement, the bank instituted a dedicated cybersecurity department.

Commanding the helm of this new department is the Chief Information Security Officer (CISO). The CISO, assisted by two (2) deputies, orchestrates the bank's cybersecurity roadmap, supervises budget allocation, and assures the alignment of cybersecurity endeavors with the bank's overarching aspirations. This dynamic trio collaboratively ensures that cybersecurity stays paramount in ACRB's strategy, with the CISO directly updating the CIO, the CEO and the Board of directors.

Within this new security realm, the Security Operations Center (SOC) stands out as a bulwark. A twelve-member team (12), split across different shifts, guards ACRB's digital frontiers round the clock. This unit is the first line of defense, swiftly identifying threats, initiating immediate countermeasures, and keeping the bank apprised of the security landscape.

Running parallel to the SOC is a team of four (4) cybersecurity analysts. These experts continuously scrutinize the bank's security fabric, making sure defenses remain up-to-date. They carry the mantle of performing regular vulnerability assessments and penetration tests to gauge the robustness of ACRB's digital infrastructure.

In the dire eventuality of a breach, an elite force of four (4), constituting the Incident Response Team, springs into action. They are also joined by four (4) existing staff from other cybersecurity teams to help them to manage incidents. This squad is tailored for rapid response, ensuring minimal damage during live threats. They periodically revisit the incident response strategy, making refinements, and frequently conduct drills to stay battle-ready.

Considering the human-centric nature of many cyber threats, ACRB has instituted a Cybersecurity Training and Awareness Team, comprising three (3) dedicated professionals, transferred from IT. This team is on a perennial mission to enlighten ACRB's workforce on the nuances of digital safety. Regular workshops, training modules, and simulated cyber-attacks form the core of their curriculum.

Compliance is non-negotiable. Ensuring this principle is the IT Compliance and Audit team of two (2). This unit guarantees that all cybersecurity maneuvers remain within the bounds of regulatory frameworks. They actively engage with external audit entities, redress IT audit observations, and make certain ACRB is perpetually primed for regulatory scrutiny.

In the ever-evolving cyberspace, staying updated is paramount. Undertaking this critical reconnaissance is the Threat Intelligence and Research Team, comprising four (4) sharp minds. Their analysis and findings empower ACRB to preemptively bolster its defenses against emerging cyber menaces.

As technology gets intricately woven into ACRB's operations, a Cybersecurity Solutions Architects (1) ensure that security remains intrinsic to every digital venture. The architect is the bridge between cybersecurity and broader IT undertakings, liaising with other internal teams and external tech vendors.

Acknowledging the proliferation of third-party digital platforms in banking, ACRB has an two-member (2) Vendor Risk Management team. Their mandate is exhaustive scrutiny

of external partners, ensuring they meet or exceed ACRB's stringent cybersecurity criteria.

The meticulous composition of these teams, with a cumulative strength of 39 experts, encapsulates ACRB's renewed commitment to cybersecurity. This multifaceted approach, spanning prevention to recovery, underscores the bank's undiluted dedication to protecting its customers, assets, and its hard-earned prestige. The total staffing budget for the newly created cybersecurity group is CAD$ 4,5 million per year, including benefits.

Description of the attack at the Atlantic Canada Regional Bank

In 2022, ACRB fell victim to a sophisticated and targeted cyber-attack, revealing several vulnerabilities within its IT infrastructure. This allowed unauthorized access, resulting in both a significant data breach and extensive financial and reputational consequences for the bank.

The attackers used spear-phishing, with several ACRB employees receiving emails appearing to originate from legitimate bank vendors or regulators. These deceptive emails contained malicious links and attachments. When unsuspecting employees clicked or opened these, they unintentionally initiated the deployment of malware within the bank's systems.

The malicious software had a dual nature: it was ransomware, which encrypted essential data, making many services unusable, and it was also equipped to exfiltrate sensitive customer data. Before its encryption activity began, the malware lay undetected for two weeks. This dormant period provided the cybercriminals with ample opportunity to explore the bank’s system and collect valuable information.

As a result of the attack, sensitive data from over 100,000 customers was exposed. This included their names, addresses, social security numbers, account balances, and transaction histories. ACRB's immediate financial damage was estimated at CAD $2

million. However, this was just the beginning. The bank grappled with the dilemma of whether to pay a significant ransom to decrypt their systems. Further costs loomed, including potential regulatory fines, compensation for affected customers, and increased cybersecurity investment.

Operationally, the bank faced a week of downtime. Critical systems were rendered inoperable, interrupting ATMs, online banking, and in-branch operations. The breach made headlines locally, eroding trust among the bank's clientele and community, particularly due to the perceived delay in notifying customers.

In response to the breach, ACRB initiated its incident protocol. They sought to isolate compromised systems and prevent further infiltration. The bank informed affected customers, liaised with regulators, and reported the incident to law enforcement. To understand the depth of the breach and get recommendations for future security, ACRB also hired a third-party cybersecurity firm.

ACRB's CEO, Peter J. Smith, and CIO, Michael L. Ross, were suspended pending an investigation, while the CFO, Myriam McDonalds, was named interim CEO. A CISO position was created, reporting directly to the Board of Directors and its Audit Committee. Elizabeth Balmoral, who had a senior leadership position in a large Canadian bank in Toronto, but wanted to return to her hometown of Halifax, was hired for this new position. The bank launched an external audit to review its cybersecurity protocols. It promised to review and strengthen its security protocols to ensure this never happens

again.

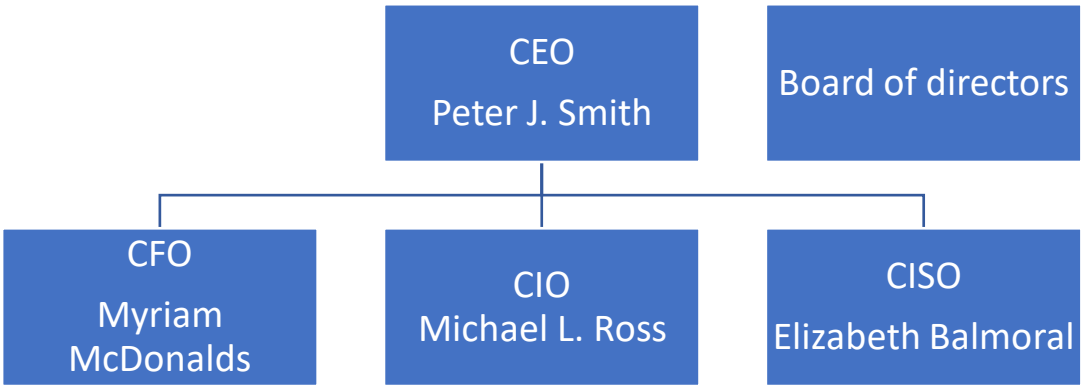

Figure 1: ACRB executive team org chart

The cyber-attack awakened ACRB, emphasizing the need for regular cybersecurity training for its employees. After all, the breach was initiated due to a successful spear-phishing attempt. This incident illustrates the need for a proactive stance on cybersecurity. It stressed the importance of periodic penetration tests, comprehensive incident response plans, and well-thought-out public relations strategies for handling such crises. This unfortunate event at ACRB serves as a poignant reminder: no entity, regardless of its size, is immune to today's complex and ever-changing cyber threat landscape.

What happened after the event

Following the 2022 cyberattack, Atlantic Canada Regional Bank (ACRB) took decisive steps to address and rebound from the situation. Immediately after detecting the attack, ACRB activated its incident response team, comprising IT specialists, cybersecurity experts, and senior bank managers. This group initiated the containment, eradication, and recovery efforts.

Recognizing the severity of the breach, the bank quickly engaged external cybersecurity firms, GoSecurity, to assist in the investigation and mitigation processes. ACRB adopted a stance of transparency and openness, proactively informing all stakeholders, such as

customers, employees, board members, regulatory bodies, and the public about the breach. To help affected customers, the bank offered credit monitoring services and offered guidance on protective steps they should consider taking.

In collaboration with GoSecurity, a deep forensic analysis was carried out to understand the breach's root cause, its scope, and the extent of the data compromise. This analysis spurred a comprehensive review of ACRB's entire IT infrastructure, identifying vulnerabilities and outdated systems that needed attention.

Moreover, adhering to Canada's banking and data protection regulations, ACRB formally reported the breach to the relevant authorities. They detailed the incident, described the bank's immediate response, and highlighted plans to prevent similar incidents in the future.

ACRB also recognized human error potential in cybersecurity incidents. In response, the bank rolled out organization-wide cybersecurity awareness and training programs. Beyond internal measures, ACRB took an in-depth look at its third-party vendors, revisiting contracts and ensuring they adhered to the bank's heightened security standards.

In the wake of the incident, the bank significantly bolstered its investment in cybersecurity infrastructure, tools, and personnel, starting with the hiring of the new CISO. The event also catalyzed the bank's long-term strategy. As soon as she arrived, the new CISO, set in motion the scenario-based cybersecurity risk assessments, which would shape ACRB's cybersecurity action plan from 2024 to 2027. This is the project that students reading this business case are tasked with performing.

For customers who faced financial losses due to compromised data, ACRB provided restitution. The bank also pursued legal action against the culprits, reinforcing their commitment to security and justice. Throughout this challenging period, ACRB's

overarching aim was to regain trust, establish robust cybersecurity practices, and be well-prepared to fend off potential future threats.

ACRB's risk appetite

As mentioned in the case, ACRB has recently suffered a significant cyber-attack in 2022. The fact that they decided to conduct a scenario-based cybersecurity risk assessment post-attack indicates that they are now prioritizing their security posture and wish to understand and address vulnerabilities.

ACRB's risk tolerance appears to be moving towards a more risk-averse posture. While they might have been more risk-neutral or even slightly risk-seeking before the incident given the vulnerabilities and lack of preparedness exhibited during the cyber-attack, the aftermath of the attack has prompted a shift in their stance. Most financial institutions, especially after suffering an attack, tend to lean heavily towards being risk-averse due to the potential financial, reputational, and regulatory implications of security breaches. ACRB's current risk tolerance at around 0.3. This rating signifies that they are highly risk-averse, but still open to some level of risk if it's aligned with potential rewards, such as implementing innovative banking solutions that might carry some degree of risk but also offer a competitive advantage.

Initial cybersecurity risk scenarios developed for ACRB

This section presents 100 cybersecurity risk scenarios that can be used with the case, when used to introduce students to cybersecurity risk assessments. These scenarios are not fully developed, so that students can use them as a starting point. The first ten (10) scenarios were fully developed and are presented in the next section.

1. Inadequate Firewall Protection: Legacy firewall fails to detect modern-day threats, allowing attackers easy ingress.
2. Employee Insider Threat: Disgruntled employee intentionally leaks confidential client data to competitors.
3. Mobile Banking App Flaw: Vulnerability in the bank's mobile app allows unauthorized access to client accounts.
4. Physical Security Breach: Unauthorized person gains access to the bank's data center due to lax security checks.
5. Obsolete Encryption Standards: Older, now-cracked encryption methods are still in use, putting data transmissions at risk.
6. Third-party Vendor Weakness: A software vendor's weak security allows backdoor access to the bank's systems.
7. Lax BYOD Policy: An employee's infected personal device connects to the bank network, spreading malware.
8. Ransomware Lockdown: Critical bank data is encrypted by ransomware, with attackers demanding payment.
9. Ineffective Incident Response: Delayed response to a detected threat results in greater damage and data loss.
10. Unpatched Software Exploit: Known vulnerabilities in unpatched software get exploited, compromising data.
11. Cloud Misconfiguration: Incorrectly configured cloud storage buckets expose sensitive bank data to the public.

12. IoT Vulnerability: Smart devices in bank premises are hacked, serving as entry points for attackers.
13. Weak Password Policies: Employees using easily guessable passwords lead to unauthorized account access.
14. Social Engineering Attack: An attacker impersonates bank staff to gather sensitive information from clients.
15. Legacy System Exploitation: Continued use of outdated systems becomes an easy target for cybercriminals.
16. DDoS Attack: Bank's online services are disrupted, causing downtime and loss of business.
17. Database Injection Attack: Attackers exploit vulnerabilities to manipulate and steal data from bank databases.
18. VPN Exploit: A vulnerability in the bank's VPN allows unauthorized remote access.
19. Misleading SSL Certificates: Users are tricked into accessing fake bank websites, compromising their credentials.
20. AI-driven Attack: Advanced AI tools predict the bank's security responses and effectively bypass them.
21. Mismanaged User Access Rights: Employees have more access than needed, increasing the potential data breach scope.
22. ATM Malware: Local ATMs infected with malware, stealing card data from bank customers.
23. Keylogging Software: Malicious software records keystrokes, capturing passwords and sensitive data.
24. Man-in-the-middle Attack: Attackers intercept and manipulate communication between the bank and its clients.
25. Data Destruction: Cyberattack results in the deletion of critical bank financial records.

26. Malicious Insider Collaboration: Employees collaborate with external actors for financial gain, compromising bank operations.
27. Uncontrolled Use of Shadow IT: Employees use unsanctioned software, introducing vulnerabilities.
28. Data Misuse by AI Algorithms: AI tools misinterpret data, causing faulty financial predictions and decisions.
29. Inadequate Audit Trails: Lack of proper logging allows malicious activities to go undetected.
30. Unsecured API Endpoints: Weak security on bank's APIs allows unauthorized data access.
31. Mobile Device Data Leak: Lost/stolen employee mobile devices give attackers access to bank's internal communication.
32. Outdated Backup Protocols: Old backup methods don't secure data properly, leading to potential breaches.
33. Insecure Wireless Networks: Wi-Fi networks at bank branches are exploited due to weak encryption.
34. Uncontrolled Admin Privileges: Too many employees have admin rights, widening the threat landscape.
35. Voice Phishing (Vishing): Scammers use phone calls to extract sensitive info from unsuspecting bank clients.
36. Malicious Chatbots: Customer support chatbots are hacked to mislead customers.
37. Compromised Biometric Data: Biometric authentication data gets exposed, jeopardizing multifactor authentication.
38. Hardware Tampering: Physical tampering of bank's servers' results in data compromise.
39. Insecure Code Deployment: Software deployed without proper security checks introduces vulnerabilities.

40. Client-side Scripting Attack: Client web browsers are targeted to steal session cookies.
41. Malicious Firmware Updates: Hardware devices receive rogue updates, causing malfunctions and data leaks.
42. Data Exfiltration via Printers: Networked printers are used as points to siphon out data.
43. Weak Security Training Programs: Employees are ill-prepared for modern threats due to outdated training.
44. Exploitation of Virtual Assistants: Voice-activated assistants on devices leak confidential conversations.
45. Rogue Mobile Banking Apps: Fake banking apps on app stores deceive users into compromising their data.
46. Inadequate Network Segmentation: Attack on one network segment easily spreads due to lack of isolation.
47. Webcam Surveillance: Webcams on bank's premises get hacked, compromising physical security.
48. Insufficient Data Masking: Sensitive data is insufficiently masked during testing, leading to potential leaks.
49. Clickjacking Attacks: Users are tricked into clicking hidden links, compromising their banking session.
50. Cryptojacking Malware: Bank's computer resources are hijacked to mine cryptocurrency, degrading performance.
51. Endpoint Protection Failure: Devices accessing the bank network lack adequate security, leading to potential breaches.
52. Spoofed Internal Communications: Attackers mimic internal email addresses, spreading misinformation or malware.
53. Server Room Environment Anomaly: Unmonitored temperature or humidity spikes damage server equipment.

54. Outdated Security Certificates: Expired SSL/TLS certificates erode trust and expose data in transit.
55. Blind Spots in Network Monitoring: Parts of the bank's network lack monitoring, allowing stealthy cyberattacks.
56. Digital Skimming Attacks: Attackers capture client data during online transactions.
57. Weakness in Two-Factor Authentication: 2FA mechanisms get bypassed due to flaws or social engineering.
58. Watering Hole Attack: Websites frequented by bank employees are compromised to target the bank's network.
59. Insufficient Patch Management: Delays in updating critical software leave systems vulnerable.
60. Third-party Data Handling Mishaps: External partners mishandle ACRB's sensitive data due to lax protocols.
61. Cryptographic Weakness: laws in cryptographic methods expose encrypted data.
62. Session Hijacking: Attackers take over user sessions to gain unauthorized access.
63. Data Hoarding: Employees or systems accumulate excessive data, amplifying breach impacts.
64. Post-breach Data Sale: Stolen bank data is sold on the dark web, leading to secondary attacks.
65. Unregulated Use of USB Drives: USB devices introduce or extract malicious content.
66. Customer Data Modification: Unauthorized changes to customer financial data lead to monetary losses.
67. Resource Exhaustion Attack: System resources are overloaded, causing service outages.
68. Misleading Domain Names: Domains resembling ACRB's lure customers into giving away their data.

69. Fileless Malware Attack: Malware residing in memory evades traditional detection mechanisms.
70. IoT Device Eavesdropping: Internet-connected devices capture and transmit confidential conversations.
71. Supply Chain Software Compromise: Software sourced from vendors contains pre-installed malware.
72. Remote Desktop Protocol (RDP) Exploits: RDP vulnerabilities provide backdoors for unauthorized access.
73. Exposure from Previous Breaches: Data from old breaches is used to launch new, targeted attacks.
74. Machine Learning Model Manipulation: ACRB's AI models are tampered with, leading to flawed outcomes.
75. DNS Cache Poisoning: Users are redirected to malicious websites when accessing ACRB's site.
76. Fraudulent Account Creation: Automated bots create fake accounts for money laundering.
77. Customer-facing Application Bugs: Flaws in user applications expose or compromise client data.
78. Misconfigured Security Groups: Incorrect permissions give users undue access to sensitive systems.
79. Misdirected Emails: Emails containing sensitive data are accidentally sent to the wrong recipients.
80. Misuse of Corporate Social Media: ACRB's social media accounts are hijacked, spreading false information.
81. Exploits via Obsolete Hardware: Old, unsupported hardware serves as a gateway for cyberattacks.
82. Proxy Server Manipulation: Bank's proxy servers are compromised, exposing user activities.

83. Digital Certificate Compromise: Stolen or forged certificates erode the trust of online platforms.

84. Unintended Data Sharing: Cloud configurations inadvertently expose data to unauthorized users.

85. Cross-site Scripting (XSS) Attack: Malicious scripts are injected into webpages viewed by bank users.

86. Data Backdoor Exfiltration: Hidden paths in systems allow data theft without detection.

87. Mobile Device Man-in-the-middle Attack: Banking apps on mobile devices get intercepted, compromising transactions.

88. Improper Data Sanitization: Old hardware, like hard drives, is discarded with retrievable data.

89. Inadequate Intrusion Detection Systems: IDS fails to identify new or sophisticated breach attempts.

90. Automated Teller Machine (ATM) Firmware Attack: Rogue firmware updates on ATMs compromise card data.

91. Malicious Insider Collaboration with External Threats: Employees secretly work with cybercriminals for data theft.

92. Shared Service Vulnerabilities: Shared IT services between branches have flaws, allowing lateral movement by attackers.

93. Replay Attacks: Authentic data transmissions are maliciously retransmitted or delayed.

94. Security Misinformation Among Staff: Employees follow outdated or misleading security advice.

95. Personal Device Compromise at Work: Personal apps or data on employee devices lead to corporate data exposure.

96. Wearable Tech Vulnerabilities: Smartwatches or fitness trackers used by staff are targeted for data interception.

97. Client-side Security Flaws: Bank's client applications lack adequate local security controls.

98. Compromised Virtual Environments: Virtualized IT environments in the bank are infiltrated.

99. Unauthorized Database Snapshot: Malicious snapshots of databases are taken for offline attacks.

100. Lack of Redundancy in Security Systems: Single points of failure in security infrastructure led to prolonged exposure.

Detailed scenarios examples

This section presents 10 cybersecurity risk scenarios that can be used with the ACRB case, when used to complete a cybersecurity risk assessment. These ten scenarios are fully developed, so that students can use them as a starting point to create a risk assessment with the methodology used in my courses.

After generating the scenarios in ChatGPT, they were expanded from the summary versions in the previous section. The query used in chatGPT was:

> *Expand the cybersecurity risk scenario « **name of scenario** » for ACRB into detailed case studies, with Scenario Name, List of stakeholders involved, Background information, Description of the scenario or incident, Event sequence, Consequences, Historical data and Mitigation and prevention. Include the Probability that the threat will be present, Probability of exploitation, Estimated expected damages, Maximal damages, Level of organizational resilience, and Expected utility on a scale of 0 to 1, calculate the CVSS score of the vulnerabilities and provide the details of the calculation. Include a budgetary estimate for the costs of implementing the mitigation and prevention measures and indicate the impact reduction and probability reduction on a scale of 0 to 1.*

Scenario 1

Scenario Name: Inadequate Firewall Protection at ACRB

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB Clients (individuals, businesses)
4. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
5. Vendors and Partners involved in ACRB's digital operations

Background Information:

Firewalls are an organization's first line of defense against potential cyber threats. However, they must be appropriately configured, monitored, and updated to effectively ward off threats.

Description of the Scenario or Incident:

ACRB's firewall was found to be using outdated protocols and lacked proper configurations, leaving it susceptible to sophisticated attacks from external threats, potentially exposing sensitive data and systems.

Event Sequence:

1. ACRB's firewall misses an irregular traffic pattern due to its outdated configurations.
2. Cybercriminals detect vulnerabilities in the firewall during a routine scan.
3. The bank's database gets infiltrated, bypassing the firewall unnoticed.
4. Malicious software gets implanted to monitor transactional data.
5. An IT team member discovers the breach during a quarterly review.

Consequences:

1. Financial Loss due to unauthorized transactions.

2. Reputational Damage to ACRB.
3. Loss of client trust and potential litigation.
4. Regulatory scrutiny and potential fines.
5. The cost of emergency cybersecurity measures and forensic investigations.

Historical Data:

In past incidents globally, almost 20% of breaches in financial institutions were due to inadequate network security, including poorly configured firewalls.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.4
- **Probability of exploitation:** 0.7
- **Estimated expected damages:** 0.6
- **Maximal damages:** 0.85
- **Level of organizational resilience:** 0.5
- **Expected utility (or Loss):** 0.168 (Calculated as 0.4 x 0.7 x 0.6)

CVSS Score Calculation Details:

- Attack Vector (AV): Network – Score: 0.85
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): None – Score: 0.85
- Scope (S): Changed – Score: 1.0
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): High – Score: 0.56

Using the CVSS 3.1 formula: Base Score is approximately 8.8 (High)

Mitigation and Prevention:

1. **Firewall Upgrade:** Install state-of-the-art firewall with advanced threat intelligence. **Cost:** $50,000 setup.
2. **Regular Firewall Audits:** Monthly firewall health checks and protocol updates. **Cost:** $25,000 annually.
3. **Network Monitoring:** Use network monitoring solutions to identify irregular traffic patterns. **Cost:** $30,000 setup + $10,000 annually.
4. **Employee Training:** Training IT staff on firewall best practices. **Cost:** $15,000 annually.
5. **Incident Response Plan:** Develop a comprehensive incident response plan specific to firewall breaches. **Cost:** $20,000.

Total Initial Cost: $145,000

Annual Maintenance: $50,000

Probability and Impact Reduction Post-Mitigation:

- Probability Reduction: From 0.75 to 0.2 (a drop of 0.55)
- Impact Reduction: From 0.9 to 0.3 (a drop of 0.6)

Scenario 2

Scenario Name: Employee Insider Threat at ACRB

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB Clients (individuals, businesses)
4. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
5. Affected third-party partners or businesses

Background Information:

The banking sector has always been a prime target for insider threats due to the value and sensitivity of the information and assets they handle. Despite trust in employees, the risk from within is undeniable.

Description of the Scenario or Incident:

A disgruntled employee with significant access rights within ACRB's system, resentful over denied promotion, decided to exploit their inside knowledge for revenge, potentially causing financial damage to the bank.

Event Sequence:

1. Disgruntled employee gets more isolated from their team.
2. Begins probing for vulnerabilities using their legitimate credentials.
3. Finds a way to manipulate transaction data to divert funds.
4. Begins siphoning moderate amounts from several accounts, directing them to dummy accounts.
5. Sets up means to launder the stolen funds.
6. The suspicious activity gets flagged during a routine system check.

Consequences:

1. Financial Loss from unauthorized transactions.
2. Reputational Damage to ACRB.
3. Regulatory scrutiny and potential fines.
4. Operational disruption due to internal investigations.

Historical Data:

About 15% of all financial institution breaches worldwide involve some form of insider participation.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.5
- **Probability of exploitation:** 0.65
- **Estimated expected damages:** 0.55
- **Maximal damages:** 0.8
- **Level of organizational resilience:** 0.6
- **Expected utility (or Loss):** 0.17925 (Calculated as 0.5 x 0.65 x 0.55)

CVSS Score Calculation Details:

- Attack Vector (AV): Local – Score: 0.5
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): High – Score: 0.27
- User Interaction (UI): None – Score: 0.85
- Scope (S): Unchanged – Score: 0.0
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Medium – Score: 0.4

Using the CVSS 3.1 formula: **Base Score** is approximately **6.8** (Medium)

Mitigation and Prevention:

1. **Regular System Audits:** Continuous IT system audits to identify any discrepancies early. **Cost:** $30,000 annually.
2. **Employee Monitoring:** Enhanced monitoring software. **Cost:** $20,000 setup + $5,000 annually.
3. **Training:** Boost employee ethical training and awareness programs. **Cost:** $15,000 annually.
4. **Multi-factor Authentication:** Reinforce all sensitive operations. **Cost:** $10,000 setup + $2,000 annually.
5. **Access Control:** Revise and restrict data access. **Cost:** $8,000 setup.

Total Initial Cost: $83,000

Annual Maintenance: $52,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.7 to 0.2 (a drop of 0.5)
- Probability Reduction: From 0.4 to 0.1 (a drop of 0.3)

Scenario 3

Scenario Name: Mobile Banking App Flaw at ACRB

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB Clients (using mobile banking services)
4. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
5. App Development and Maintenance Vendors
6. Third-party integration providers (like payment gateways)

Background Information:

Mobile banking apps have surged in popularity due to their convenience. With increased use, the security of these apps is of utmost importance to safeguard user data and financial transactions.

Description of the Scenario or Incident:

A vulnerability in ACRB's mobile banking app was identified, potentially allowing malicious actors to intercept sensitive user data, including login credentials and transaction details.

Event Sequence:

1. An independent security researcher, during a routine security analysis, discovers a flaw in the app's encryption mechanism.
2. Exploiting the flaw, a malicious actor could initiate man-in-the-middle attacks.
3. Users report unauthorized transactions, raising alarms in the bank's fraud department.
4. ACRB IT team confirms the vulnerability and rushes to release a patch.

Consequences:

1. Financial loss from unauthorized transactions.
2. Reputational damage to ACRB.
3. Decreased trust in ACRB's digital platforms by users.
4. Legal implications and potential fines.
5. Costs associated with rectifying the unauthorized transactions and compensating affected users.

Historical Data:

In the past few years, around 18% of financial institutions worldwide have reported vulnerabilities in their mobile applications, leading to potential security breaches.

CVSS Score Calculation Details:

- Attack Vector (AV): Network – Score: 0.85
- Attack Complexity (AC): Medium – Score: 0.66
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): Required – Score: 0.62
- Scope (S): Changed – Score: 1.0
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Medium – Score: 0.4

Using the CVSS 3.1 formula: Base Score is approximately 8.6 (High)

Mitigation and Prevention:

1. **App Patch:** Immediate patch to fix the identified vulnerability. **Cost:** $40,000.
2. **Enhanced Encryption:** Upgrade the app's encryption mechanisms. **Cost:** $30,000 setup.

3. **Regular App Audits:** Quarterly security checks for the mobile app. **Cost:** $20,000 annually.
4. **User Notification & Training:** Inform users about the importance of updating their apps and safe online practices. **Cost:** $10,000 annually.
5. **Incident Response Protocol:** Develop a specific protocol for app-related breaches. **Cost:** $15,000.

Total Initial Cost: $115,000

Annual Maintenance: $30,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.8 to 0.2 (a drop of 0.6)
- Probability Reduction: From 0.6 to 0.15 (a drop of 0.45)

Scenario 4

Scenario Name: Physical Security Breach at ACRB

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. Employees and personnel working at ACRB facilities
4. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
5. Security service providers contracted by ACRB
6. ACRB clients

Background Information:

While cyber threats dominate the narrative in modern banking security, physical breaches—such as unauthorized access to data centers, banking premises, or computer systems—remain a tangible risk. Adequate physical safeguards are essential to prevent data theft, sabotage, or espionage.

Description of the Scenario or Incident:

An unauthorized individual gains physical access to ACRB's primary data center by exploiting weaknesses in perimeter security and tailgating employees. Once inside, the individual attempts to install surveillance devices and exfiltrate sensitive data directly from servers.

Event Sequence:

1. The intruder observes staff movements and identifies lax security protocols.
2. They tailgate an employee through a security checkpoint without being stopped.
3. Using basic electronic tools, the intruder accesses a secure server room.
4. Surveillance devices are placed, and data is copied onto portable storage devices.

5. The breach is discovered two days later during a routine security audit.

Consequences:

1. Potential data theft, leading to exposure of sensitive customer data.
2. Reputational damage to ACRB.
3. Loss of trust from clients and partners.
4. Legal and regulatory consequences, including potential fines.
5. The cost of forensic investigation and breach remediation.

Historical Data:

Physical security breaches at financial institutions, though less frequent than cyber incidents, have accounted for approximately 8% of total security incidents in the banking sector over the past five years.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.25
- **Probability of exploitation:** 0.4
- **Estimated expected damages:** 0.75
- **Maximal damages:** 0.85
- **Level of organizational resilience:** 0.6
- **Expected utility (or Loss):** 0.075 (Calculated as 0.25 x 0.4 x 0.75)

CVSS Score Calculation Details: (Note: CVSS is typically used for software vulnerabilities; however, for the sake of this exercise, we can try to approximate):

- Attack Vector (AV): Physical – Score: 0.2
- Attack Complexity (AC): High – Score: 0.44
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): None – Score: 0.85
- Scope (S): Changed – Score: 1.0

- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Medium – Score: 0.4

Using the CVSS 3.1 formula: **Base Score** is approximately **5.6** (Medium)

Mitigation and Prevention:

1. **Enhanced Perimeter Security:** Upgrade fences, access points, and add surveillance. **Cost:** $100,000 setup.
2. **Advanced Access Control:** Implement biometric access controls for sensitive areas. **Cost:** $75,000 setup.
3. **Regular Security Audits:** Monthly physical security checks. **Cost:** $10,000 annually.
4. **Staff Training:** Training on security protocols and threat identification. **Cost:** $20,000 annually.
5. **Incident Response Plan:** Protocol for physical security incidents. **Cost:** $15,000.

Total Initial Cost: $210,000

Annual Maintenance: $30,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.75 to 0.2 (a reduction of 0.55)
- Probability Reduction: From 0.4 to 0.1 (a reduction of 0.3)

Scenario 5

Scenario Name: Obsolete Encryption Standards at ACRB

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB's customers and clients
4. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
5. Third-party technology vendors
6. External cybersecurity consultants

Background Information:

Encryption is a cornerstone of data protection and privacy. With the advancement of computational power and sophisticated algorithms, older encryption standards can become obsolete and more susceptible to decryption attempts by malicious actors.

Description of the Scenario or Incident:

ACRB is discovered to be using outdated encryption standards for its online banking transactions, putting all electronic data transfers, including sensitive customer information, at risk.

Event Sequence:

1. An external security researcher identifies and reports the obsolete encryption standard after testing ACRB's online banking portal.
2. A hacker group becomes aware of this vulnerability and begins targeting ACRB's online transactions.
3. Multiple unauthorized decryption attempts are detected by ACRB's cybersecurity team.

4. Immediate patchwork is applied to secure transactions while a solution is sought.
5. Investigation confirms several instances of data exposure.

Consequences:

1. Potential compromise of sensitive customer transaction data.
2. Reputational damage to ACRB.
3. Trust erosion among the bank's clients.
4. Legal ramifications and potential regulatory fines.
5. Costs associated with damage control, customer notifications, and potential compensations.

Historical Data:

In recent years, a decline in organizations using obsolete encryption has been observed. However, about 4% of financial institutions globally were found to have some exposure due to outdated encryption practices in the last two years.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.2
- **Probability of exploitation:** 0.6
- **Estimated expected damages:** 0.8
- **Maximal damages:** 0.95
- **Level of organizational resilience:** 0.55
- **Expected utility (or Loss):** 0.096 (Calculated as 0.2 x 0.6 x 0.8)

CVSS Score Calculation Details:

- Attack Vector (AV): Network – Score: 0.85
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): None – Score: 0.85

- User Interaction (UI): None – Score: 0.85
- Scope (S): Unchanged – Score: 1.0
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Low – Score: 0.29

Using the CVSS 3.1 formula: **Base Score** is approximately **7.5** (High)

Mitigation and Prevention:

1. **Immediate Encryption Upgrade:** Shift to the latest industry-standard encryption protocols for all data transmission. **Cost:** $150,000.
2. **Ongoing Encryption Review:** Quarterly reviews to ensure encryption standards are up-to-date. **Cost:** $40,000 annually.
3. **Employee Training:** Updated training programs for IT staff on maintaining and verifying security protocols. **Cost:** $25,000 annually.
4. **External Security Audits:** Annual external audits to identify vulnerabilities. **Cost:** $50,000 annually.
5. **Incident Response Strategy:** Detailed protocols for any future breaches. **Cost:** $20,000.

Total Initial Cost: $220,000

Annual Maintenance: $115,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.8 to 0.2 (a reduction of 0.6)
- Probability Reduction: From 0.5 to 0.1 (a reduction of 0.4)

Scenario 6

Scenario Name: Third-party Vendor Weakness at ACRB

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB's customers and clients
4. Third-party technology vendors
5. External cybersecurity consultants
6. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)

Background Information:

ACRB relies on various third-party vendors for specialized services, such as cloud storage solutions, transaction processing systems, and customer relationship management software. While these third-party solutions can provide cost-effective and efficient services, they can also introduce potential vulnerabilities if not properly managed or if the vendor itself has weak security practices.

Description of the Scenario or Incident:

A third-party payment processing vendor utilized by ACRB has a security vulnerability in its software. Unbeknownst to ACRB, this vulnerability has exposed sensitive financial data of thousands of ACRB's customers.

Event Sequence:

1. The vulnerability in the third-party software is discovered and sold on the dark web.
2. Malicious actors exploit the vulnerability, accessing sensitive transaction data.
3. Suspicious transaction activities are reported by ACRB's customers.
4. ACRB's IT team traces the breach back to the third-party vendor's software.

5. The vendor is notified, and emergency patches are applied.

Consequences:

1. Leak of sensitive customer data, including account details and transaction histories.
2. Reputational damage to ACRB, with a loss of trust among customers.
3. Legal implications and potential regulatory fines due to data breach.
4. Financial losses from potential fraudulent transactions.
5. Costs associated with forensic investigations, customer notifications, and compensations.

Historical Data:

In the last five years, around 60% of data breaches in the financial sector have been linked to vulnerabilities from third-party vendors.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.6
- **Probability of exploitation:** 0.5
- **Estimated expected damages:** 0.85
- **Maximal damages:** 0.95
- **Level of organizational resilience:** 0.6
- **Expected utility (or Loss):** 0.255 (Calculated as 0.6 x 0.5 x 0.85)

CVSS Score Calculation Details:

- Attack Vector (AV): Network – Score: 0.85
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): None – Score: 0.85
- Scope (S): Changed – Score: 1.08

- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Medium – Score: 0.42

Using the CVSS 3.1 formula: **Base Score** is approximately **8.0** (High)

Mitigation and Prevention:

1. **Vendor Security Assessment:** Before onboarding, assess and approve the security protocols of any third-party vendor. **Cost:** $100,000.
2. **Regular Security Audits:** Perform bi-annual security audits of all third-party services in use. **Cost:** $70,000 annually.
3. **Contractual Agreements:** Ensure that all vendor contracts include clauses for regular security updates and liability in case of breaches. **Cost:** Minimal, included in legal overheads.
4. **Internal Monitoring Systems:** Enhance internal security monitoring systems to detect vulnerabilities from third-party integrations faster. **Cost:** $50,000.
5. **Incident Response Strategy:** Develop a specific response plan for third-party vulnerabilities. **Cost:** $30,000.

Total Initial Cost: $180,000

Annual Maintenance: $100,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.9 to 0.3 (a reduction of 0.6)
- Probability Reduction: From 0.6 to 0.2 (a reduction of 0.4)

Scenario 7

Scenario Name:

Lax Bring Your Own Device (BYOD) Policy at Atlantic Canada Regional Bank (ACRB)

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB Employees
4. ACRB's customers and clients
5. External cybersecurity consultants
6. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)

Background Information:

ACRB allows employees to use their personal devices for work-related activities to promote flexibility and ease of access. While this can boost employee satisfaction and productivity, a lax BYOD policy can also introduce significant security vulnerabilities.

Description of the Scenario or Incident:

An employee at ACRB accessed sensitive client financial data using their personal tablet, which had minimal security features. The tablet was later compromised when the employee clicked on a malicious link from a personal email, leading to unauthorized access to ACRB's internal network.

Event Sequence:

1. Employee uses a personal tablet to access ACRB's secure files and client data.
2. The employee, while using the tablet for personal browsing, inadvertently clicks on a phishing link.
3. Malware is installed on the device, which seeks out and exploits the connection to ACRB's network.

4. Unauthorized access to sensitive data and potential data exfiltration occur.
5. ACRB IT detects unusual network activity and initiates an investigation.

Consequences:

1. Breach of confidential client data.
2. Potential financial fraud if the data is used maliciously.
3. Reputational damage to ACRB.
4. Legal implications and potential fines.
5. Costs associated with forensic investigations, data recovery, and client notifications.

Historical Data:

As of 2021, approximately 30% of companies have experienced a data breach as a result of insecure personal devices.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.4
- **Probability of exploitation:** 0.3
- **Estimated expected damages:** 0.7
- **Maximal damages:** 0.9
- **Level of organizational resilience:** 0.5
- **Expected utility (or Loss):** 0.084 (Calculated as 0.4 x 0.3 x 0.7)

CVSS Score Calculation Details:

- Attack Vector (AV): Local – Score: 0.55
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): Required – Score: 0.62
- Scope (S): Changed – Score: 1.08

- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Medium – Score: 0.42

Using the CVSS 3.1 formula, the **Base Score** is approximately **7.5** (High).

Mitigation and Prevention:

1. **BYOD Policy Revision:** Strengthen the BYOD policy with specific security requirements. **Cost:** $5,000.
2. **Employee Training:** Offer regular training sessions on secure BYOD practices. **Cost:** $20,000 annually.
3. **Device Security Software:** Mandate and subsidize the installation of security software on all personal devices used for work. **Cost:** $30,000 annually.
4. **Regular Device Audits:** Conduct bi-annual audits of personal devices to ensure compliance. **Cost:** $15,000 annually.
5. **Multi-factor Authentication:** Implement MFA for access to ACRB's internal systems from personal devices. **Cost:** $25,000.

Total Initial Cost: $75,000

Annual Maintenance: $65,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.8 to 0.3 (a reduction of 0.5)
- Probability Reduction: From 0.7 to 0.2 (a reduction of 0.5)

Scenario 8

Scenario Name:

Ransomware Lockdown at Atlantic Canada Regional Bank (ACRB)

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB's employees across all departments and branches
4. ACRB's customers and clients
5. External cybersecurity consultants and forensic experts
6. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
7. Media and general public

Background Information:

Ransomware attacks have surged in the last decade, targeting institutions of all sizes, including banks. With attackers becoming more sophisticated and demanding significant ransoms, institutions must ensure robust cybersecurity measures are in place.

Description of the Scenario or Incident:

An attacker successfully installs ransomware on ACRB's central server, encrypting critical financial data and rendering core banking systems inoperative. A ransom note demands $2 million in cryptocurrency in exchange for the decryption key.

Event Sequence:

1. ACRB employee receives a phishing email and unknowingly downloads a malicious attachment.
2. The ransomware spreads through the internal network, targeting the bank's central servers.
3. Critical systems become inoperable, and the ransom note is displayed.

4. The IT team is alerted to the attack and begins to assess the situation.
5. Senior management convenes an emergency meeting to determine the next steps.

Consequences:

1. Temporary suspension of ACRB banking services.
2. Potential loss of critical data, including financial records.
3. Significant financial cost if the ransom is paid.
4. Reputational damage leading to loss of customer trust.
5. Potential regulatory fines and legal consequences.
6. Costs associated with restoring systems and data recovery.

Historical Data:

As of 2021, ransomware attacks resulted in an average downtime of 21 days for affected organizations, with an average ransom payment of $312,493.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.5
- **Probability of exploitation:** 0.4
- **Estimated expected damages:** 0.85
- **Maximal damages:** 0.95
- **Level of organizational resilience:** 0.4
- **Expected utility (or Loss):** 0.17 (Calculated as 0.5 x 0.4 x 0.85)

CVSS Score Calculation Details:

- Attack Vector (AV): Network – Score: 0.85
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): Required – Score: 0.62

- Scope (S): Changed – Score: 1.08
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): High – Score: 0.56

Using the CVSS 3.1 formula, the **Base Score** is approximately **8.6** (High).

Mitigation and Prevention:

1. **Backup Systems:** Ensure regular, isolated backups of all critical data. **Cost:** $50,000 annually.
2. **Employee Training:** Conduct quarterly cybersecurity awareness training focusing on phishing attacks. **Cost:** $30,000 annually.
3. **Advanced Threat Detection:** Implement a solution for detecting and mitigating advanced threats. **Cost:** $60,000.
4. **Network Segmentation:** Isolate critical systems to prevent the spread of malware. **Cost:** $45,000.
5. **Email Security Solutions:** Implement advanced email filtering solutions to reduce the chances of malicious emails reaching employees. **Cost:** $25,000 annually.

Total Initial Cost: $175,000

Annual Maintenance: $105,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.9 to 0.4 (a reduction of 0.5)
- Probability Reduction: From 0.8 to 0.3 (a reduction of 0.5)

Scenario 9

Scenario Name: Ineffective Incident Response at Atlantic Canada Regional Bank (ACRB)

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB's employees across all departments and branches
4. ACRB's customers and clients
5. External cybersecurity consultants and forensic experts
6. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
7. Media and general public

Background Information:

Incident response is the approach an organization takes to manage the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. An effective incident response plan can mitigate damage, recover lost data, and restore system functionality for continuity of business operations.

Description of the Scenario or Incident:

A malware attack infiltrates the bank's mainframe and begins exfiltrating data to an unknown external server. The ACRB's cybersecurity team, lacking an established incident response plan, struggles to coordinate an effective response.

Event Sequence:

1. Anomalous network traffic is identified by the bank's monitoring system.
2. The cybersecurity team is notified but struggles to diagnose the issue due to lack of preparation and expertise.
3. Malware is discovered on the mainframe, and data is seen being sent to an unknown external IP.

4. Management is informed, but no immediate action plan is in place.
5. The cybersecurity team attempts to isolate the affected system without a clear procedure, causing further disruptions.
6. The incident becomes public knowledge, and ACRB faces backlash from customers and regulators.

Consequences:

1. Data breach involving sensitive customer data.
2. System downtime, impacting banking operations.
3. Reputational damage causing loss of customer trust and potential withdrawals.
4. Regulatory fines due to non-compliance and poor incident handling.
5. Increased costs related to post-incident investigations, customer compensations, and public relations efforts.

Historical Data:

As of 2021, the average time to identify a breach was 207 days, and the average time to contain a breach was 73 days. These durations could be significantly reduced with an effective incident response plan.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.6
- **Probability of exploitation:** 0.5
- **Estimated expected damages:** 0.8
- **Maximal damages:** 0.9
- **Level of organizational resilience:** 0.3
- **Expected utility (or Loss):** 0.24 (Calculated as 0.6 x 0.5 x 0.8)

CVSS Score Calculation Details:

- Attack Vector (AV): Network – Score: 0.85

- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): Low – Score: 0.68
- User Interaction (UI): None – Score: 0.85
- Scope (S): Changed – Score: 1.08
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): High – Score: 0.56

Using the CVSS 3.1 formula, the **Base Score** is approximately **8.4** (High).

Mitigation and Prevention:

1. **Incident Response Plan Development:** A detailed and updated plan that covers all potential scenarios. **Cost:** $40,000.
2. **Cybersecurity Training:** Regular training sessions for the cybersecurity team on the latest threats and mitigation techniques. **Cost:** $20,000 annually.
3. **Incident Response Drills:** Quarterly drills to simulate potential threats and test the effectiveness of the response plan. **Cost:** $15,000 annually.
4. **External Consultation:** Employ external cybersecurity consultants to periodically review and update the incident response plan. **Cost:** $30,000 annually.
5. **Advanced Monitoring Solutions:** Implement monitoring solutions that can rapidly detect and alert on anomalies. **Cost:** $50,000 with an annual maintenance of $10,000.

Total Initial Cost: $135,000

Annual Maintenance: $75,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.8 to 0.4 (a reduction of 0.4)
- Probability Reduction: From 0.7 to 0.3 (a reduction of 0.4)

Scenario 10

Scenario Name:

Unpatched Software Exploit at Atlantic Canada Regional Bank (ACRB)

List of Stakeholders Involved:

1. ACRB Senior Management & Board of Directors
2. ACRB IT & Cybersecurity Team
3. ACRB's employees across all departments and branches
4. ACRB's customers and clients
5. Software vendors
6. Regulatory Authorities (e.g., Banking Regulation Agency of Canada)
7. Media and general public

Background Information:

Unpatched software presents a significant vulnerability, with many cyberattacks leveraging known vulnerabilities in widely used software applications. Keeping software updated and patched is critical for cybersecurity.

Description of the Scenario or Incident:

The bank's core banking software contains an unpatched vulnerability. Malicious actors discover and exploit the vulnerability, gaining unauthorized access to sensitive financial data.

Event Sequence:

1. A known vulnerability is announced by the software vendor, with patches available for the flaw.
2. Due to oversight, ACRB's IT team doesn't prioritize the patch.
3. Cybercriminals detect ACRB's exposure and target the bank.
4. Unauthorized data access is accomplished.

5. Suspicious activities alert the internal cybersecurity team.
6. Investigations confirm a breach, with data potentially exfiltrated.

Consequences:

1. Unauthorized access to confidential customer financial data.
2. Possible financial losses if transactions are manipulated.
3. Reputational damage leading to loss of customer trust.
4. Regulatory scrutiny and potential fines.
5. Cost of remediation, including potential compensation to affected customers.

Historical Data:

As of 2021, studies indicated that 60% of breaches involved vulnerabilities for which a patch was available but not applied. The time between vulnerability disclosure and the first exploitation attempt had decreased, with cybercriminals acting faster than ever before.

Key risk indicator metrics :

- **Probability that the threat will be present:** 0.7
- **Probability of exploitation:** 0.6
- **Estimated expected damages:** 0.8
- **Maximal damages:** 0.9
- **Level of organizational resilience:** 0.4
- **Expected utility (or Loss):** 0.336 (Calculated as 0.7 x 0.6 x 0.8)

CVSS Score Calculation Details:

- Attack Vector (AV): Local – Score: 0.55
- Attack Complexity (AC): Low – Score: 0.77
- Privileges Required (PR): None – Score: 0.85
- User Interaction (UI): None – Score: 0.85

- Scope (S): Changed – Score: 1.08
- Confidentiality Impact (C): High – Score: 0.56
- Integrity Impact (I): High – Score: 0.56
- Availability Impact (A): Medium – Score: 0.42

Using the CVSS 3.1 formula, the **Base Score** is approximately **7.8** (High).

Mitigation and Prevention:

1. **Patch Management Solution:** Automated tools to track, test, and apply patches. **Cost:** $50,000 with an annual maintenance of $5,000.
2. **Regular Vulnerability Assessments:** Monthly scans and assessments to find and rectify vulnerabilities. **Cost:** $25,000 annually.
3. **Employee Training:** Educate IT staff about the importance of timely patching. **Cost:** $10,000 annually.
4. **External Audits:** Annual third-party security audits to ensure compliance and identify weak spots. **Cost:** $30,000 annually.
5. **Backup Solutions:** Ensure robust and regular backups to recover data if needed. **Cost:** $20,000 initial setup and $5,000 annual maintenance.

Total Initial Cost: $125,000

Annual Maintenance: $75,000

Impact and Probability Reduction Post-Mitigation:

- Impact Reduction: From 0.9 to 0.5 (a reduction of 0.4)
- Probability Reduction: From 0.8 to 0.4 (a reduction of 0.4)