**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ACRB's firewall was found to be using outdated protocols and lacked proper configurations, leaving it susceptible to sophisticated attacks from external threats, potentially exposing sensitive data and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 ACRB's firewall misses an irregular traffic pattern due to its outdated configurations.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)