**Creating cybersecurity risk scenarios with ChatGPT, a tutorial.**

**By Marc-André Léger, PhD**

**November 30th 2023**

This article presents an approach to accelerate the creation of cybersecurity risk scenarios using generative AI.

**Introduction**

Artificial intelligence models, such as ChatGPT, create interesting opportunities for cybersecurity scenario modeling. It aligns well with the rapid advancements we are witnessing in artificial intelligence and cybersecurity applications. Here, I will present a proposal on how ChatGPT and similar models can be harnessed to accelerate cybersecurity risk scenario creation.

To begin, it's important to recognize that the cybersecurity landscape is vast and evolving. Threat vectors change, and attack patterns adjust based on technological advancements and organizational behavior shifts. For cybersecurity risk analysts and researchers, keeping up with the myriad of potential scenarios is challenging.

ChatGPT and similar large-scale language models can consume vast amounts of textual information and comprehend context to a significant extent. By leveraging the ability to use large amounts of data, one can accelerate the generation and understanding of potential risk scenarios.

One of the promising uses of ChatGPT in cybersecurity risk modeling is scenario generation. Given a set of input parameters or contexts, such as a specific network architecture or application configuration, ChatGPT can generate multiple potential risk scenarios. These can be based on historical data, known vulnerabilities, or emerging threats documented in the literature and other sources.

Cybersecurity is dynamic, meaning new vulnerabilities, attack vectors, and patterns emerge frequently. With every update or iteration of models like ChatGPT, they can be trained on new data. This ensures that the generated scenarios remain relevant and up-to-date.

For a researcher or cybersecurity analyst, searching through a plethora of sources to understand a potential risk can be time-consuming. ChatGPT can synthesize information from multiple sources, providing a comprehensive understanding of a risk scenario.

While ChatGPT generates scenarios, it's equally crucial to validate them. ChatGPT can help validate generated scenarios with the available literature, providing a level of confidence or likelihood for each scenario.

Beyond risk modeling, ChatGPT can be used in cybersecurity training and awareness programs. It can generate potential attack or breach scenarios for mock drills, aiding in real-time training and ensuring organizational teams are prepared for diverse challenges.

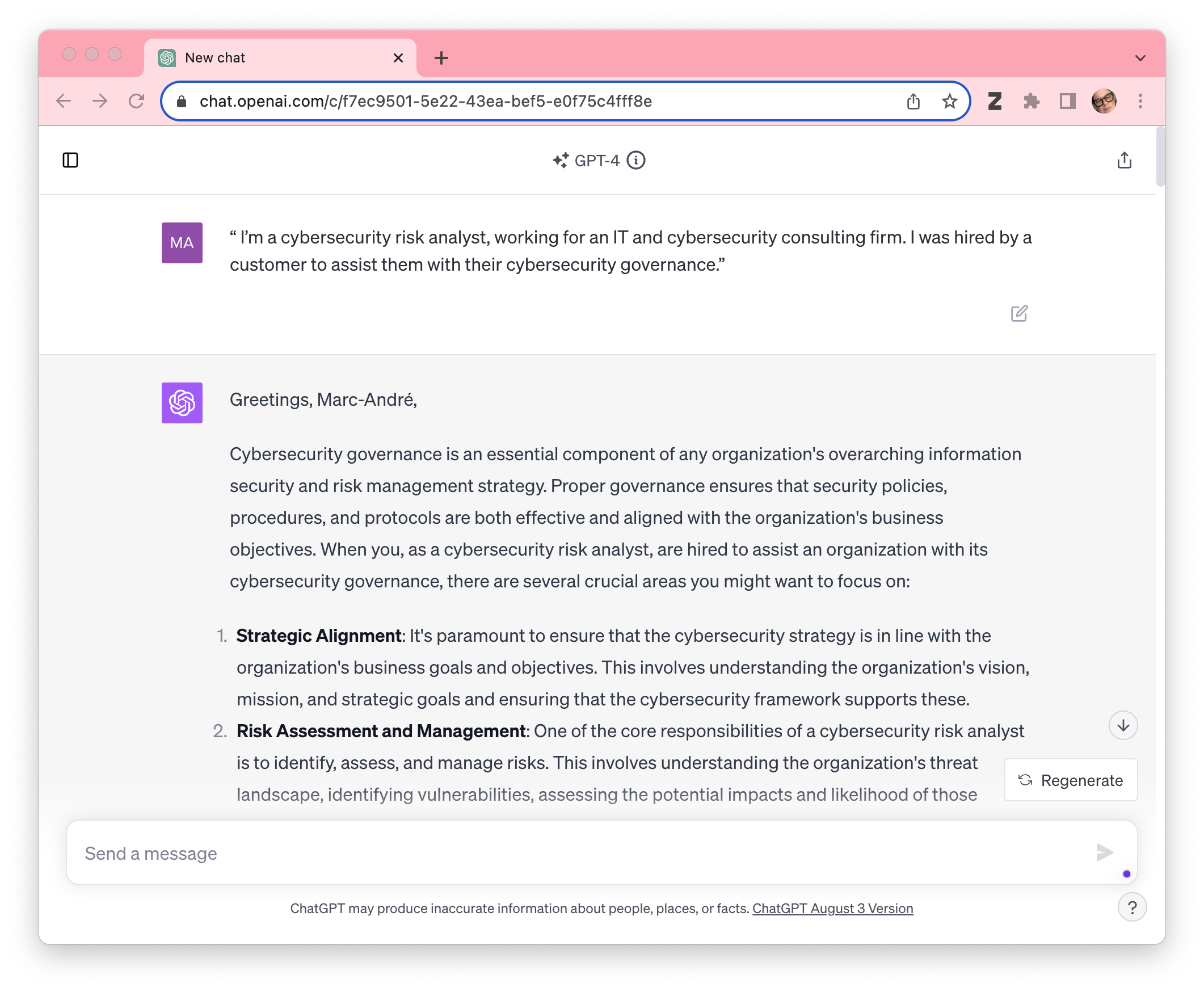
**Creating scenarios**

The first thing you need to do is to teach ChatGPT about the organization. In this article we are using the business case create by Marc-André Léger intitled A Scenario-based cybersecurity risk assessment for the Atlantic Canada Regional Bank, made available to students on Moodle. Please note that this case is about a fictious organization. The case itself was generated with the help of ChatGPT as well. It is also available here : <https://www.researchgate.net/publication/373953728_Business_Case_A_Scenario-based_cybersecurity_risk_assessment_for_the_Atlantic_Canada_Regional_Bank>

**Step 1: provide context.**

Open ChatGPT and select the GPT-4 model, if available to you. Otherwise, you can use the most advanced version you have access to. First, provide some context to ChatGPT. Open a **New Chat** and enter the following information:

*“I’m a cybersecurity risk analyst, working for an IT and cybersecurity consulting firm. I was hired by a customer to assist them with their cybersecurity governance.”*



Then paste the following information from the business case to teach the tool about the organization you which to generate cybersecurity risk scenarios.

*« Here is what you need to know about the target organization we will be using: 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.*

*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).*

*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.*

*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. 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. 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. 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. ACRB provides various digital platforms including an online Banking Portal, Mobile Banking App, ATMs, and Point of sale (POS) terminals. »*

**Step 2: create high-lev scenarios**

Then you can create a list of cybersecurity risk with the following prompt:

*Create 50 cybersecurity risk scenario for ACRB.*

The result is presented in appendix A.

**Step 3: create detailed scenarios**

Finally, create detailed risk scenarios with the following prompt:

*Expand the cybersecurity risk scenario* ***NAME OF THE SCENARIO*** *at ACRB into a detailed cybersecurity risk scenario, with the Scenario Name, a List of the stakeholders involved, some Background information out the scenario, a detailed Description of the scenario or the incident leading to the undesired outcome, a bullet list of Event sequence, a description of the Consequences, some Historical data and proposed Mitigation measures, internal controls and prevention mechanisms. On a scale of 0 to 1, Include the Probability that the threat will be present, the Probability of exploitation, the Estimated expected damages, the Maximal damages, the Level of organizational resilience, and the Expected utility. All of these need to be on a scale of 0 to 1. Then, calculate the CVSS version 3.1 score of the vulnerabilities and provide the details of the calculation. Include a budgetary estimate for the costs of implementing the proposed Mitigation measures, internal controls and prevention mechanisms. Indicate the impact reduction and probability reduction on a scale of 0 to 1 for the proposed Mitigation measures, internal controls and prevention mechanisms.*

The resulting output is presented in appendix B. The result of what is presented in the detailed scenario should be reviewed for a real-word use. For our use, in a classroom setting, they will be used as is to perform a cybersecurity risk assessment, using the method that is presented in class.

**Conclusion**

While there's undeniable potential in using ChatGPT for cybersecurity risk scenarios, it's crucial to proceed with caution. Reliance on artificial intelligence should not overshadow human judgment and expertise. Cybersecurity has nuances and complexities that require human intervention. ChatGPT models must be considered for potential biases or inaccuracies. As well, current versions are limited by training data a few years old. For example, the training data in the currently available ChatGPT version is from September 2021.

In conclusion, as information technology and cybersecurity evolve, the fusion of artificial intelligence tools and techniques with traditional methods presents an opportunity for enhanced efficiency and capability. ChatGPT models are used in cybersecurity risk scenario modeling testifies to this potential. It promises accelerated scenario generation but also a comprehensive, updated, and synthesized view of potential risks. This ensures that researchers, analysts, and organizations remain a step ahead in the ever-evolving cyber threat landscape.

**Appendix A: results from the 50 scenatios**

Given the details you've provided about ACRB, here are 50 cybersecurity risk scenarios for the bank:

1. **Phishing Campaign**: Employees at various branches receive phishing emails attempting to steal their credentials.
2. **ATM Skimming**: Unauthorized devices installed on ACRB's ATMs to collect card data from unsuspecting customers.
3. **Legacy System Vulnerability**: An outdated component in the core banking system becomes exploited.
4. **Cloud Misconfiguration**: Incorrect settings on AWS or Azure lead to data exposure.
5. **Ransomware Attack**: Malicious software encrypts ACRB's critical data, demanding a ransom for release.
6. **Insider Threat**: A disgruntled employee deliberately leaks sensitive customer data.
7. **VPN Exploitation**: A vulnerability in the VPN solution connecting branches is exploited, providing unauthorized access.
8. **Unpatched Software**: An unpatched piece of software on a server leads to a security breach.
9. **Mobile Banking App Vulnerability**: A security flaw in the mobile app exposes customer credentials.
10. **DDoS Attack**: ACRB's online banking portal becomes targeted by a distributed denial-of-service attack, causing a service outage.
11. **POS Terminal Tampering**: A point-of-sale terminal in a branch gets compromised, capturing customer card data.
12. **Physical Data Center Breach**: Unauthorized individuals gain physical access to one of the data centers.
13. **Supplier Vulnerability**: A third-party software used by ACRB contains a security flaw that's exploited.
14. **Weak Encryption**: Data in transit is captured and decrypted due to weak encryption standards.
15. **Social Engineering**: A branch manager is tricked into releasing sensitive information over the phone.
16. **Data Leakage**: Customer data is accidentally uploaded to a public cloud storage bucket.
17. **Backup Failure**: The bank's backups fail to restore after a critical system failure.
18. **IoT Device Exploitation**: A smart device in a branch, such as a thermostat or security camera, is exploited as an entry point.
19. **Inadequate Access Controls**: An employee accesses data they shouldn't be able to due to misconfigured permissions.
20. **Outdated Firewall Rules**: Old firewall configurations allow malicious traffic into the network.
21. **AI Data Poisoning**: The AI-driven data analytics tool receives manipulated data, leading to flawed insights.
22. **Employee Credential Sharing**: Two employees share login credentials, leading to account misuse.
23. **Lack of Multi-Factor Authentication**: An account is breached as it only relies on a password without a second authentication factor.
24. **Patch Management Delays**: A crucial update is delayed, leaving systems vulnerable for an extended period.
25. **Biometric Bypass**: Biometric security measures at a branch are bypassed using sophisticated techniques.
26. **Third-party Vendor Breach**: A vendor with access to ACRB's data experiences a security breach.
27. **Malicious Insider**: An employee intentionally plants malware within the bank's infrastructure.
28. **Weak Password Policies**: Employees use easily guessable passwords, leading to unauthorized access.
29. **Stolen Laptops**: Laptops with sensitive information are stolen from a branch.
30. **Unsecured APIs**: The bank's application programming interfaces (APIs) are exploited due to inadequate security measures.
31. **Disgruntled Ex-employee Access**: An employee who was recently terminated still has access to critical systems.
32. **Data Center Outage**: A natural disaster causes an unexpected outage at one of the data centers.
33. **Spoofed Banking Portal**: A fake version of ACRB's online portal is created to steal customer credentials.
34. **Unsecured Wireless Networks**: Unauthorized access to ACRB's network through weak wireless security at a branch.
35. **Man-in-the-Middle Attack**: Communication between a branch and the main data center is intercepted.
36. **Database Injection**: The bank's database is exploited through an SQL injection attack.
37. **Inadequate Incident Response**: A breach occurs, and due to inadequate response protocols, it escalates.
38. **Failure to Detect Intrusion**: The intrusion detection system fails to identify a breach in real-time.
39. **Stolen Backup Drives**: Physical backup drives are stolen from a data center.
40. **Remote Access Exploitation**: Unauthorized remote access is gained due to weak remote access policies.
41. **Unintended Data Sharing**: Customer data is unintentionally shared with third parties due to misconfigurations.
42. **Third-party Software Flaws**: A third-party software used by ACRB introduces vulnerabilities.
43. **Data Mismanagement**: Sensitive data is stored without proper encryption or protection measures.
44. **Outdated Endpoint Protection**: Anti-virus and anti-malware solutions on endpoints become outdated and fail to detect a new threat.
45. **Malicious Mobile App**: A fake ACRB mobile app is distributed, targeting the bank's customers.
46. **Unsafe Development Practices**: Developers introduce vulnerabilities due to a lack of secure coding practices.
47. **Misconfigured IDS/IPS**: Intrusion detection and prevention systems are misconfigured, leading to missed detections.
48. **Compromised Vendor Credentials**: Malicious actors gain access to ACRB's systems using stolen vendor credentials.
49. **Exposure from Previous Breaches**: Data from a past breach is used to launch a targeted attack against ACRB customers.
50. **Mismanaged End-of-Life Hardware**: Outdated hardware that's no longer supported introduces vulnerabilities to the network.

These scenarios represent a mix of technical and human-oriented risks, highlighting the multifaceted nature of cybersecurity challenges ACRB might face. Proper risk assessment and mitigation strategies should be developed for each scenario.

**Appendix 2 : example of the detailed scenario for Ransomware Attack**

Given the information, here's a detailed expansion on the ransomware attack scenario for ACRB:

**Scenario Name**: Ransomware Attack on ACRB’s IT Infrastructure

**Stakeholders Involved**:

* ACRB IT Team
* ACRB Cybersecurity Team
* ACRB Executive Management
* ACRB Customers
* Regulators
* Third-party cybersecurity vendors

**Background**: ACRB, due to its recent adoption of modern digital banking tools and legacy systems, can be seen as a prime target for ransomware attacks. The financial gain for attackers and the bank's critical position in Atlantic Canada makes it crucial for ACRB to defend against such threats.

**Description**: A sophisticated ransomware variant infects ACRB's IT systems. This malware encrypts critical data, rendering systems non-functional and preventing access to essential banking services, both offline and online. The attacker demands a substantial amount in cryptocurrency for the decryption key.

**Event Sequence**:

* An employee inadvertently opens a phishing email and downloads a malicious attachment.
* The malware spreads laterally within the network.
* Critical systems and databases become encrypted.
* A ransom note appears on affected systems, demanding payment.
* ACRB's IT and Cybersecurity teams are alerted.
* Communication is established between the attacker and ACRB.

**Consequences**:

* Interruption of banking services, including online banking.
* Loss of trust among customers.
* Potential financial loss if a decision to pay the ransom is made.
* Regulatory fines and penalties due to potential data breaches.
* Increased cybersecurity and PR costs in the aftermath.

**Historical Data**: In recent years, several banks worldwide have fallen victim to ransomware attacks, with varying levels of impact. Some chose to pay the ransom, while others opted to restore systems from backups.

**Mitigation Measures, Internal Controls, and Prevention Mechanisms**:

* Regular backups and their testing.
* Employee cybersecurity awareness training.
* Endpoint detection and response systems.
* Network segmentation.
* Threat hunting and regular vulnerability assessments.
* Multi-factor authentication.

**Budgetary Estimate**:

* Training: $50,000 annually
* Endpoint solutions: $200,000 (licenses, deployment)
* Regular backups: $100,000 annually
* Vulnerability assessments: $75,000 annually
* Total: $425,000 initially, with ongoing costs per year.

**Impact Reduction for Mitigation**:

* Regular backups: 0.8
* Employee training: 0.5
* Endpoint solutions: 0.7
* Network segmentation: 0.6
* Threat hunting and assessments: 0.7

**Probability Reduction for Mitigation**:

* Regular backups: 0.6
* Employee training: 0.7
* Endpoint solutions: 0.8
* Network segmentation: 0.7
* Threat hunting and assessments: 0.7

**Risk Metrics**:

* Probability that the threat will be present: 0.7
* Probability of exploitation: 0.6
* Estimated expected damages: 0.6
* Maximal damages: 0.9
* Level of organizational resilience: 0.5
* Expected utility: 0.6

**CVSS v3.1 Calculation**:

* **Attack Vector**: Local (L)
* **Attack Complexity**: Low (L)
* **Privileges Required**: None (N)
* **User Interaction**: Required (R)
* **Scope**: Changed (C)
* **Confidentiality Impact**: High (H)
* **Integrity Impact**: High (H)
* **Availability Impact**: High (H)
* **Exploit Code Maturity**: High (H)
* **Remediation Level**: Official Fix (O)
* **Report Confidence**: Confirmed (C)

Based on the above metrics, the CVSS Base Score would be approximately 8.6, indicating a high severity.