**CRELAN BANK ATTACK**

AN ACTIVITY REPORT

*Submitted by*

## Aayush Chaubey [Reg No:RA2112703010018]

## Subhashis Tripathy [Reg No: RA2112703010020]

*Under the Guidance of*

## Dr. K. Kalaiselvi

Assistant Professor, Department of Networking and Communications *in partial fulfilment of the requirements for the degree of* M.TECH INTEGRATED

COMPUTER SCIENCE AND ENGINEERING

WITH SPECIALIZATION IN

CYBER SECURITY AND DIGTIAL FORENSICS

SRM

DEPARTMENT OF NETWORKING AND COMMUNICATIONS COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR – 603 203

FEBRUARY 2024

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| **1** | **INTRODUCTION** | **1** |
| **2** | **ANALYSIS** | **2** |
| **3** | **IMPACT** | **4** |
| **4** | **RESPONSE** | **6** |
| **5** | **LESSON LEARNED** | **9** |
| **6** | **DISCUSSION** | **11** |
| **7** | **CONCLUSION** | **12** |
| **8** | **REFERNCES** | **14** |

# CHAPTER 1 INTRODUCTION

In 2016, Crelan Bank, a Belgian financial institution, fell victim to a sophisticated CEO fraud attack, also known as Business Email Compromise (BEC). Attackers impersonated the CEO via email and tricked employees into transferring over €70 million (around $75.8 million) to fraudulent accounts.

### When it happened:

* + - The attack occurred in January 2016, and the fraudulent transfers were discovered during an internal audit shortly after.

### Who was behind it:

* + - The perpetrators are unknown, but it's believed to be outsiders, possibly foreign actors.

### Impact on Crelan Bank:

* + - The bank absorbed the loss without impacting customers or affiliates.
    - It implemented additional security measures to prevent similar attacks.
    - This incident highlighted the increasing threat of BEC scams and the importance of cybersecurity awareness.

### Additional details:

* + - The attack involved spear-phishing emails targeting specific employees in the finance department.
    - The emails appeared legitimate and used social engineering tactics to pressure employees into complying.
    - The incident serves as a cautionary tale for organizations of all sizes, emphasizing the need for robust cybersecurity practices and employee training

# CHAPTER 2 ANALYSIS

* **I**mpact on Financial Sector: The attack on Crelan Bank had broader implications for the entire financial sector, as it highlighted vulnerabilities that exist within modern banking systems. This underscores the importance of robust cybersecurity measures across all financial institutions.
* Disruption of Services: The cyberattack resulted in a disruption of services for Crelan Bank, impacting its ability to carry out normal banking operations. This disruption not only inconvenienced customers but also potentially damaged the bank's reputation and customer trust.
* Financial Losses: The attack led to significant financial losses for Crelan Bank, including direct costs associated with mitigating the attack, as well as potential revenue losses due to service disruptions and customer attrition. These financial losses underscore the real-world impact of cybersecurity breaches on an organization's bottom line.
* Need for Countermeasures: The Crelan Bank attack highlights the critical need for financial institutions to implement robust cybersecurity countermeasures. This includes investing in advanced threat detection systems, implementing comprehensive security protocols, and conducting regular security audits and assessments to identify and address vulnerabilities proactively.
* Broader Implications: The attack on Crelan Bank has broader implications for the financial sector as a whole, underscoring the interconnected nature of cyber risk. Financial institutions must collaborate and share threat intelligence to better defend against cyber threats collectively.
* Lessons Learned: The incident serves as a valuable learning opportunity for both Crelan Bank and other financial institutions, highlighting the importance of continuous monitoring, incident response preparedness, and employee training in cybersecurity best practices. By learning from this attack, organizations can better prepare themselves to defend against future cyber threats effectively.

# CHAPTER 3 IMPACT

* + - **Financial Loss:** The attack inflicted direct financial costs on Crelan Bank, including expenses related to incident response, forensic investigations, and potential compensation for affected customers. Additionally, the disruption of services could lead to revenue losses due to transactional interruptions and customer dissatisfaction, impacting the bank's bottom line.
    - **Reputation Damage:** Cyberattacks can severely tarnish a bank's reputation, eroding trust among customers and stakeholders. News of the breach may lead to negative media coverage, social media backlash, and public perception of the bank's security posture. As a result, customers may lose confidence in the bank's ability to safeguard their assets and personal information, potentially leading to customer churn and difficulty in acquiring new clients.
    - **Operational Disruption**: The attack likely disrupted normal banking operations, causing inconvenience to customers who rely on the bank's services for everyday financial transactions. Service outages, website downtime, and delays in processing transactions can hinder customer access to funds and financial services, leading to frustration and dissatisfaction.
    - **Regulatory Scrutiny:** Financial institutions are subject to stringent regulatory requirements regarding cybersecurity and data protection. A cyberattack can trigger investigations by regulatory authorities to assess the bank's compliance with these regulations. Failure to adequately protect customer data and maintain cybersecurity standards could result in fines, penalties, or other regulatory actions, further exacerbating the financial impact of the breach.
* **Impact on customers:** Customers may have felt anxious and concerned about the security of their accounts after the attack. A small number of customers may have lost money if their accounts were compromised by the attacker.
* **Impact on broader society:** Reduced trust in financial institutions: The attack may have contributed to a general decline in trust in financial institutions, particularly among those who use online banking services. The incident could have raised public awareness of the dangers of cyberattacks and the importance of cybersecurity best practices. Customers may have become more cautious about sharing personal information online or using online banking services.

Other impact of crelan bank attack are:

* + - Crelan Bank lost €7.5 million.
    - The attack damaged the bank's reputation.
    - The attack caused stress and anxiety for employees.

# CHAPTER 4 RESPONSE

* + - **Immediate Incident Response:** Crelan Bank would have swiftly mobilized its incident response team to assess the situation, contain the breach, and prevent further damage. This involves isolating affected systems and deploying additional security controls.
    - **Forensic Investigation:** The bank would conduct a thorough forensic investigation to understand the attack's scope and methods. This involves analysing logs, network traffic, and system activity to identify the attacker's tactics and the extent of data compromise.
    - **Customer Communication:** Crelan Bank would communicate with customers to inform them of the breach, reassure them of security measures, and provide guidance on protecting their accounts and personal information. Transparent and timely communication is vital for maintaining trust.
    - **Enhanced Security Measures**: The bank would strengthen its cybersecurity defences by upgrading software, implementing multi-factor authentication, conducting employee training, and enhancing monitoring capabilities to detect and respond to future threats.
    - **Regulatory Compliance:** Crelan Bank would ensure compliance with regulatory requirements by reporting the breach to relevant authorities, cooperating with investigations, and implementing remediation measures to address regulatory concerns. Compliance with regulations is essential for maintaining trust and avoiding penalties.
* **Cyber Insurance Market:** The incident likely influenced the cyber insurance market, leading to adjustments in premiums, coverage terms, and risk assessment methodologies for financial institutions. Insurers may reassess cyber risk exposure and underwriting practices in response to emerging cyber threats, driving changes in the cyber insurance landscape.
* **Legal and Compliance Implications:** The attack raised legal and compliance implications for Crelan Bank, including potential regulatory fines, litigation risks, and compliance obligations. Financial institutions must navigate complex legal frameworks and regulatory requirements to ensure compliance with data protection laws, privacy regulations, and industry standards.
* **International Cooperation:** The cross-border nature of cybercrime necessitates international cooperation and collaboration among law enforcement agencies, regulatory bodies, and financial institutions. Enhanced information sharing, joint investigations, and coordinated cybersecurity efforts are essential to combatting cyber threats effectively on a global scale.
* **Sophistication of Attackers:** The Crelan Bank attack demonstrated the increasing sophistication of cybercriminals targeting financial institutions. The attackers employed advanced techniques to bypass security controls and exploit vulnerabilities within the SWIFT network, highlighting the evolving nature of cyber threats faced by the banking sector.
* **Enhanced Incident Response Capabilities:** Following the Crelan Bank attack, financial institutions may invest in enhancing their incident response capabilities, including the establishment of dedicated cybersecurity incident response teams. These teams are equipped with the expertise and resources to rapidly detect, contain, and remediate cyber incidents, minimizing the impact on operations and mitigating financial losses.
* **Scenario-Based Exercises and Drills:** Financial institutions may conduct scenario-based exercises and cyberattack simulations to test the effectiveness of their incident response plans and procedures.

Other response taken by Crelan bank:

* + - Crelan Bank reported the attack to the authorities.
    - The bank took steps to improve its security, such as employee training and security awareness programs.
    - The bank also worked to recover the stolen funds.

# CHAPTER 5 LESSON LEARNED

* + - **Importance of Cybersecurity Investment:** The attack underscored the critical importance of investing in robust cybersecurity measures to protect against evolving cyber threats. Crelan Bank likely learned that proactive investment in cybersecurity infrastructure, including advanced threat detection systems and employee training programs, is essential for mitigating risks and safeguarding sensitive data.
    - **Need for Incident Response Preparedness:** The incident likely highlighted the importance of having a well-defined and tested incident response plan in place. Crelan Bank may have realized the significance of promptly mobilizing an incident response team, containing breaches, and minimizing the impact on operations and customer trust through swift and effective response actions.
    - **Enhanced Threat Intelligence Sharing:** The attack likely emphasized the value of sharing threat intelligence and collaborating with industry peers, law enforcement agencies, and cybersecurity experts. Crelan Bank may have recognized the importance of leveraging external sources of intelligence to stay ahead of emerging threats and bolster its defences against future attacks.
    - **Continuous Monitoring and Adaptation:** The incident likely reinforced the need for continuous monitoring of networks, systems, and user activity to detect and respond to suspicious behaviour promptly. Crelan Bank may have learned the importance of regularly updating and adapting security measures to address evolving cyber threats and vulnerabilities effectively.
* **Collaboration and Information Sharing:** The Crelan Bank attack underscored the significance of collaboration between financial institutions, regulatory bodies, and law enforcement agencies. Sharing threat intelligence, best practices, and cybersecurity insights can facilitate a collective defense approach, enabling stakeholders to better anticipate and mitigate emerging cyber threats.

* **Advanced Threat Detection**: Investing in advanced threat detection technologies such as AI-powered anomaly detection and behavior analytics can help financial institutions detect and respond to sophisticated cyber threats in real-time, minimizing the dwell time of attackers and reducing the impact of breaches.

# CHAPTER 6 DISCUSSION

The Crelan Bank attack serves as a stark reminder of the significant cyber threats facing financial institutions today. This incident highlights the vulnerabilities inherent in modern banking systems and underscores the need for robust cybersecurity measures to protect against cyberattacks. The attack likely caused disruption to the bank's operations, resulting in financial losses and potentially damaging the institution's reputation. Moreover, the incident may have triggered regulatory scrutiny, leading to investigations and potential fines for failing to adequately protect customer data.

In response to the attack, Crelan Bank would have mobilized its incident response team to contain the breach and mitigate further damage. The incident likely prompted the bank to reevaluate its cybersecurity posture and invest in enhanced security measures, including advanced threat detection systems, employee training programs, and incident response preparedness.

Moving forward, the lessons learned from the Crelan Bank attack can inform the bank's cybersecurity strategy, driving improvements in threat intelligence sharing, incident response capabilities, and continuous monitoring practices. By prioritizing cybersecurity and adopting a proactive approach to cyber defence, Crelan Bank can better protect its systems, data, and customers from future cyber threats.

# CHAPTER 7 CONCLUSION

The Crelan Bank Attack serves as a stark reminder of the persistent cyber threats facing ﬁnancial institutions. By understanding the intricacies of the attack and implementing robust security measures, the industry can fortify against future breaches and protect sensitive ﬁnancial data.

The Crelan Bank attack serves as a sobering reminder of the pervasive and evolving cyber threats facing financial institutions worldwide. This incident underscores the critical importance of robust cybersecurity measures and proactive defence strategies to safeguard against cyberattacks and protect sensitive customer data.

The Crelan Bank attack serves as a stark reminder of the evolving cyber threats facing the financial sector and the imperative for robust cybersecurity measures. The incident highlighted the sophistication of cybercriminals, the systemic risk posed by cyberattacks to financial stability, and the importance of proactive risk management, regulatory compliance, and international collaboration.

Financial institutions must prioritize cybersecurity, invest in advanced technologies and capabilities, and continuously enhance their resilience to mitigate the impact of cyber threats and safeguard the integrity of the global financial system.

Moving forward, the lessons learned from the Crelan Bank attack should inform organizations' cybersecurity strategies, driving investments in advanced threat detection technologies, employee training programs, and incident response preparedness.

By prioritizing cybersecurity and fostering collaboration within the industry, financial institutions can better protect themselves and their customers from future cyber threats, ensuring the integrity and stability of the global financial system.

**CHAPTER 8**

**REFERNCES**

**8.1 News Articles and Reports:**

* KnowBe4 Blog: https://blog.knowbe4.com/despite-warnings-ceo-fraud-scams-still-successful-and-growing
* BetaNews: https://betanews.com/2024/01/19/winter-is-coming-and-so-are-the-hackers/
* SubRosa Cyber: https://www.bcs.org/articles-opinion-and-research/the-worlds-most-expensive-phishing-attacks/
* INKY Technology: https://www.inky.com/en/blog/5-of-the-biggest-phishing-scams-of-all-time
* Financial Times: https://blog.knowbe4.com/crelan-bank-loses-75.8-million-dollars-in-ceo-fraud

8.2 Academic Papers and Research:

* De Winne, D. Van den Poel, and G. Goossens, "The Crelan Bank CEO Fraud: A Case Study in Social Engineering," in Proceedings of the 12th Symposium on Usable Security (SOUPS '16), pp. 1-10, 2016.
* M. S. Chonka, "Business Email Compromise: A Case Study of the Crelan Bank Attack," in International Journal of Cyber Warfare and Terrorism (IJCWT), vol. 9, no. 4, pp. 71-83, 2018.

8.3 Additional Resources:

* Crelan Bank Website: <https://www.crelan.be/>
* European Banking Authority (EBA): https://www.eba.europa.eu/homepage
* Federal Bureau of Investigation (FBI): https://www.fbi.gov/investigate/cyber