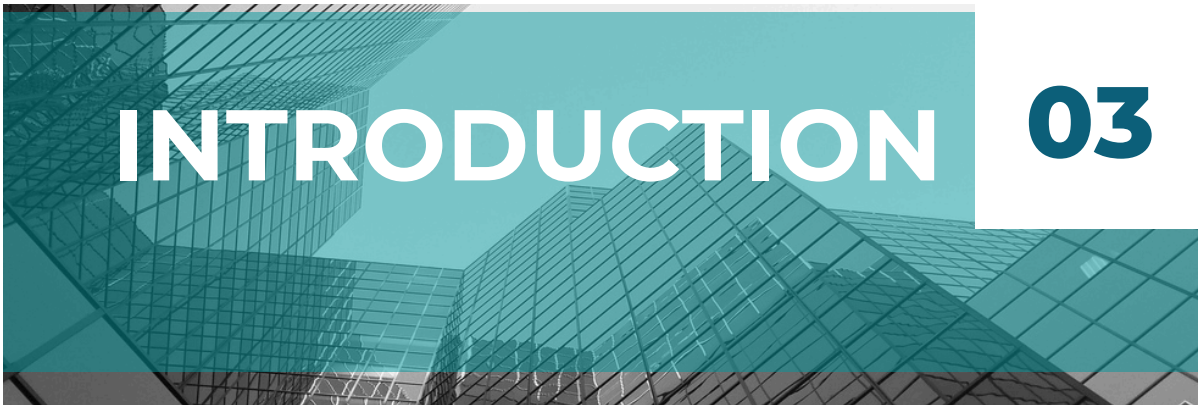
CYBERSECURITY EXCELLENCE AT TD BANK:
EMPOWERING OUR EMPLOYEES

Prepared By: Puneet Sandher
Wednesday, March 13, 2024
MGMT*3330: Project Management

TABLE OF CONTENTS



INTRODUCTION 03

TD Bank is a leading Canadian bank known for its customer service, innovative financial products, and trustworthiness. Trustworthiness and data protection are important to Canadians, especially with 78 percent of Canadians conducting their banking needs online (Canadian Banking Association, 2022). TD Bank, and other Canadian banks, must be dedicated to fostering a culture of cybersecurity awareness and data privacy. This requires the cooperation of all employees which can be introduced by hosting a comprehensive cybersecurity seminar for employees to enhance their understanding and knowledge. *Cybersecurity Excellence at TD Bank: Empowering our Employees* is a one-day seminar for TD Bank employees to gain an understanding and prioritize cybersecurity in their daily tasks. This project has four objectives: host a comprehensive and engaging event, promote safe cyber practices, develop a culture of cybersecurity awareness, and reduce cybersecurity threats at the company. These objectives will be met by keynote presentations from cybersecurity specialists and hands-on activities that will demonstrate best cyber practices with common employee tasks. The event is scheduled for April 17th, 2024 and will be hosted at the auditorium in TD Bank's downtown Toronto office, which can accommodate a maximum of 400 attendees.

To develop an understanding of the project scope and the importance of hosting this seminar, this report will highlight the crucial role of cybersecurity in the banking sector. A comprehensive analysis of the project's significance and relevance for the company, the importance of cybersecurity, and how cybersecurity will be incorporated into the seminar. An analysis of the seminar's feasibility will be conducted to highlight strengths, potential challenges, and mitigation strategies.

PROJECT SIGNIFICANCE

04

Fostering a strong cybersecurity culture is crucial for banks as it's a highly publicized topic, maintaining customers' trust, remaining compliant with federal regulations, and executing risk management. According to a study from the University of Maryland, every 39 seconds a cybersecurity attack occurs that impacts a third of Americans (IBM, 2024). Cybersecurity attacks are prevalent and are significant risks for every company, affecting millions of people each year. Moreover, cyber incidents in Canadian banking have increased significantly in the past year. In 2022, it was reported to be ten high-level cyber incidents from Canadian banks but this almost tripled in 2023 with 28 incidents that leaked private data and caused service disruptions (Tunney, 2024). Educating TD employees on the significance and severity of cyberattacks, as well as, sharing the latest data and insights in the field will help cultivate a culture of cybersecurity importance in the company.

As previously stated, the majority of customers conduct their banking online which requires a trusting relationship with their bank. A consumer analysis report by PWC found that 87 percent of consumers will sever ties with a company they do not trust to protect data (PWC, 2017). Publicly sharing efforts to promote a cybersecurity culture, such as this seminar, TD Bank can strengthen client confidence. Client confidence is vital for a bank to remain successful, especially in the current climate where all Canadian banks are struggling with cyberattacks (Nardi, 2024). TD Bank can attract clients from its competitors by focusing on becoming a trailblazer in cybersecurity in Canadian banking and publicizing these cyber-safe initiatives for all Canadians to see.

The federal government is determined to pass new cyber-safe bills to protect the data of all Canadians. Bill C-26, although pending approval, requires all businesses in finance, telecommunication, energy, and transportation to hold all cybersecurity operations within Canada (Tunney, 2024). In addition, businesses in these industries must have a system to identify cyber incidents and a system to prevent cyber incidents (Tunney, 2024). This cybersecurity seminar aligns with the government's goals of regulating and creating guidelines to promote cybersecurity practices.

05

Lastly, risk management is important for banks as they hold sensitive customer information and handle money. This seminar on cybersecurity is an example of risk prevention as employees will learn how to complete their daily tasks with cyber-safe practices in mind, as well as, create an environment of innovation where employees can share their ideas of preventing this risk. Strong risk prevention strategies for cybersecurity will protect TD Bank from potential lawsuits and protect its reputation. A cybersecurity seminar for employees will reduce the likelihood of cyberattacks, strengthen relationships with clients, remain competitive, align with future regulations, and practice risk management.

BACKGROUND AND INSIGHTS ON CYBERSECURITY

06

According to IBM, cybersecurity is the application of technology and practices to prevent and mitigate cyberattacks (IBM, 2021). Cyberattacks can lead to viruses, data leaks and compromise the privacy of electronic devices. There are five key domains in cybersecurity: critical infrastructure security, network security, endpoint security, application security, cloud security, information security, and mobile security (IBM, 2021). Businesses must address each domain of cybersecurity with a comprehensive risk management plan to guard against cyber threats. Cyberattacks put a company at risk for lawsuits, disruption to business operations, financial loss, and harm to a business's reputation. This risk is ever-evolving, and emerging. IBM's Cost of a Data Breach 2023 report found it costs 4.46 million USD to resolve a data breach and ransomware data breach was 5.13 million USD (IBM, 2021). TD Bank, as well as many other banks, hold sensitive data of millions of clients that will cost millions of dollars if a data breach were to occur.

Types of Cyberattacks

Large amount of data flows through devices and networks every second, but a cyberattack can compromise this flow. Simply, connecting devices to an organization's Wi-Fi exposes the risk of data leaks and cyberattacks. For example, smartphones have access to a person's name, password, location, and phone number and are commonly targeted as individuals connect to businesses' free Wi-Fi. There are various complex and creative types of cyber-attacks that companies and individuals need to be cautious and prepared for specifically, malware, phishing, ransomware, and distributed denial of service attacks.

Malware, or malicious software, is viruses and other harmful programs that can give unauthorized access to systems and steal data (IBM, 2021). Phishing attacks, usually disguised as emails from trusted sources, ask to share sensitive information (IBM, 2021). Ransomware is malware that holds and encrypts user data until the user pays a ransom (IBM, 2021). Distributed denial of service attacks were most prevalent during the COVID-19 pandemic and aimed to crash a network or service using high levels of traffic (IBM, 2021). These examples are examples of the overarching cyber threats each business faces and the importance of implementing comprehensive cybersecurity strategies.

07

Cybersecurity in Organizations

A comprehensive risk strategy for cybersecurity requires the use of technology, processes, and people (CISCO, 2024). There are many enterprise technical skills to assist in the monitoring and protection from cyber-attacks such as malware protection, email security, and firewalls (CISCO, 2024). Hackers hope to invade businesses through their devices, rotors, networks, and the cloud (CISCO, 2024). Employees must practice cyber-safe methods, such as strong passwords, to ensure they do not cause a security breach to occur due to reckless online behaviours (CISCO, 2024). Moreover, larger companies may have a data forensics team which can secure technological infrastructure when a cyberattack is identified. Every cyberattack will require specific mitigation practices and has a level of severity, that a business must consider in the development of its risk management process. The company must develop operations and processes to handle cyberattacks specifically to find, protect, and recover attacks (Bedrich, 2020). These processes must also include a communication plan such as employee cybersecurity education to reduce human risk, as well as, how impacted parties will be informed when an attack occurs. Overall, the collective use of available technology, cooperation of employees and a set of standards and protocols will make companies more prepared for a cyber-attack.

Cybersecurity Best Practices

The Government of Canada has an extensive list of best cybersecurity practices for businesses related to network protection, system protection, and education (Canadian Centre for Cyber Security, 2022). There is an emphasis on the development of processes and management plans for security information, incident response, network monitoring, and hardware and software equipment (Canadian Centre for Cyber Security, 2022). Moreover, companies must have risk management and cybersecurity audits to identify weaknesses and develop mitigation strategies. There are basic practices that all companies should already be following such as multi-factor authentication on system accounts, ensuring each user's privileges are essential, updating software and hardware to ensure vulnerabilities are addressed, and installing antivirus software (Canadian Centre for Cyber Security, 2022). There are ample enterprise tools available for businesses to keep their operations secure, however, recent years have been challenging. The quality and development of enterprise cybersecurity tools have been hindered due to the limited data on cyberattacks as companies do not publish incidents and their impacts (Cremer et al., 2022). Developing tools for cybersecurity using machine learning methodologies to identify cyber risks requires larger datasets, that are not currently available (Cremer et al., 2022). If businesses are legally obligated to report cyberattacks, it would innovate and improve the accuracy of current cybersecurity tools and all companies could improve their risk management plan (Deloitte, 2024). Improve cybersecurity practices for all Canadian companies, requires collaboration and transparency.

08

Difficulties Implementing Cybersecurity Practices

As stated previously there are various types of cyberattacks and the most common cause is due to human error, where an individual is unable to identify security risks (PWC, 2024). The size of a business does not dictate its probability of being targeted, however, in smaller organizations, the IT department is often responsible for cybersecurity amongst their original duties lowering the quality of cybersecurity (PWC, 2024). Cyberattacks were more frequent for employees during lockdown due to the COVID-19 pandemic as the dramatic shift did not provide companies enough time to train employees on cyber-safe practices (PWC, 2024). Lack of employee education and training left millions of companies vulnerable and many are still facing the consequences. Education is a common and effective strategy to mitigate risk as a significant amount of data breaches occur due to human error. Moreover, another potential risk mitigation strategy is investing in AI cybersecurity tools that use deep learning, machine learning and natural language processing to check for employee negligence specifically, fraud, intrusion and any abnormalities (Chamorro-Premuzic, 2023). The AI cybersecurity industry has grown rapidly and will be worth 35 billion dollars in 2025, compared to 2017's four billion dollars (Chamorro-Premuzic, 2023). This option could be a solution in the future as there are still issues with accuracy and require a significant amount of resources to implement, currently, the best solution is employee education.

Cybersecurity Practices to Prevent Human Error

Employees who are not cybersecurity specialists are at risk of compromising a company's privacy, especially due to phishing schemes (CISCO, 2023). Phishing schemes use social engineering to develop and impersonate people to lure victims to provide confidential information (CISCO, 2023). This is especially common for phishing emails to be sent to an employee's company email that can easily go unnoticed, such as an email to "verify" details of a confidential project. Moreover, some phishing schemes hold malware when the reader opens the email or opens any links in the email (CISCO, 2023). Many companies emulate phishing schemes to teach employees how to identify them and mandate a short phishing detection course for employees who fail these phishing tests. However, phishing schemes continuously innovating and it is more difficult to identify, which is why a significant amount of people fall for these schemes due to lack of exposure and human error remains a common reason for cyberattacks.

CYBERSECURITY AND THE SEMINAR

09

As previously stated, a comprehensive cybersecurity process is vital for a company's success and the greatest risk is employees who lack a foundational knowledge of cyber safety. The research proves that there is a gap in employee training, employees lack vigilance in regards to cybersecurity, and this gap must be addressed to continue TD Bank's success. *Cybersecurity Excellence at TD Bank: Empowering our Employees* has the objective of addressing these issues the company faces.

Lack of Effective Employee Training

Most companies have similar cyberattack prevention strategies that are generic and based on the statistics but are not effective. Employees' lack of diligence has caused the majority of cyberattacks. A more comprehensive and engaging cybersecurity culture is necessary, as cyberattacks and risks are an ever-evolving issue due to technological innovation. As previously stated, the transition to remote working because of the COVID-19 pandemic brought a new wave of cyberattacks, which will continue to be a relevant issue as TD Bank has now developed a hybrid working model. During the pandemic, 47 percent of employees fell for COVID-19 phishing emails while working from home (Nabe, 2020). This is due to the plethora of distractions from working from home, therefore, it is crucial to create a vigilant and concise cyber safety culture among all employees (Nabe, 2020).

According to Forbes, developing a culture of accountability and rewarding employees for doing their due diligence of improving their cyber skills and informing managers of potential threats, can lower employee-caused cyberattacks (Forbes, 2022). This seminar would introduce a phase in the company of a more focused cybersecurity culture, with the entire event based on best practices to educate employees backed by credible research. The goal of the seminar is to move past generic corporate cybersecurity online courses and use more effective strategies such as gamifying the experience. Employees will be collaborating and be given simulated daily tasks to complete that have potential cyber risks that must learn to identify and navigate, once they complete a simulation they provide to another of high difficulty. Through these activities, employees will better retain the skills they learned during the seminar and directly apply them to their job tasks.

Importance of Cybersecurity in Banking

There are many types of cyberattacks and prevention strategies that each company must integrate into their management and processes. Given the frequent evolution of best practices due to evolving technology and as more research becomes publicly available, constant vigilance is vital. Clients will work with banks they trust and demonstrate data privacy vigilance. Clients are transferring money, paying bills and doing other tasks online which require cyber-safe practices. To demonstrate competence, employees who are directly interacting with clients must be well-versed on the subject, which is many employees working at local branches and those working with high-profile clients. Currently, employees lack foundational knowledge due to a lack of company vigilance in cybersecurity practices. This seminar will educate employees on the risks of cybersecurity by having various cybersecurity experts present the dangers and answer any questions and concerns employees may have. This educational component led by industry speakers will shift employees' perspectives of cybersecurity and understand TD Bank's shift toward a more vigilant cybersecurity culture.

Costs Associated with Cybersecurity

The IBM's Cost of Data Breach report outlined the significant costs of cyberattacks, as well as, the associated costs from potential lawsuits and mitigation which can also hurt a company's future business operations. Thorough preventative measures of educating cybersecurity as this seminar intends to do will save a company a lot of money. The speaker presentations will outline the regulatory and compliance requirements, to ensure all employees are compliant to prevent any government audits and fines. Especially, as Bill C-26 could be passed soon and employees need to be aware of its existence and implications, which the speakers will handle. The project plan supports the need for addressing ongoing government regulations and understanding the severity of cyberattacks. In addition, the seminar's simulated activities are a cost-efficient option to provide an introduction to cybersecurity and company expectations, compared to the cost of real-life cyber incidents. Conducting events and initiatives related to cybersecurity will increase the employees' confidence in the company, build trust in the company as a customer and save TD Bank millions of dollars.

FEASIBILITY ASSESSMENT

11

This assessment will evaluate the project's feasibility by evaluating the overall feasibility, strengths, potential challenges, and mitigation strategies.

Feasibility

It is highly feasible to execute the *Cybersecurity Excellence at TD Bank: Empowering our Employees* seminar due to the allocated resources and TD Bank's commitment to improving its cybersecurity practices. This seminar will address cyber-safe practices, the application of these skills, developing vigilance, and the severe impacts of cyberattacks. TD Bank has an extensive cybersecurity department that can be leveraged in the consultation of the material covered in the event, as well as, the expert speakers can share specialized knowledge. The allocated budget and company resources will suffice to accomplish the project's objectives. Overall, the scope of this seminar aligns with TD Bank's goals, aligns with current industry shifts and is feasible with all the resources available.

Strengths

This seminar is an all-encompassing introduction to cybersecurity for employees of all backgrounds to learn from cybersecurity specialists to develop a foundational understanding of the concepts, their importance, and how to apply best practices in their jobs. This is in alignment with the values of TD Bank, government regulations and maintaining competitiveness through a cost-effective format. The seminar will introduce cross-departmental collaboration where employees can understand how best cybersecurity practices can be practiced in different departments, especially in a collaborative environment. This event offers an opportunity to promote shared responsibility for cyber defence and strengthen organizational cohesion. Employees will feel more confident in the leaders of the company and overall company commitment to taking initiative and direct action to improve the data privacy practices, which will improve employee retention.

12

Potential Challenges and Mitigation Strategies

There are various potential challenges during the planning and execution of the event, however, there are mitigation strategies to respond to these issues. As with all events, there are potential challenges with attendance as employees are busy or some employees may feel overly confident in their cyber practices and feel it is unnecessary to attend, which roots back to the company culture. Developing an incentive and recognition system can further a foster cybersecurity awareness culture. Moreover, many concepts must be addressed in the seminar which may be difficult to do within one working day, which will require providing concise information and removing excess information so the audience is not overwhelmed. To remain within budget and have the maximum amount of attendees, the seminar will be made relevant for all employees resulting in a more generalized knowledge and activities. This will reduce the effectiveness of the overarching goal of improving employees' cybersecurity practices, however, this is an introductory event with the potential of subsequent specialized seminars for departments. In addition, developing practical cybersecurity activities will require extensive research and consultation, especially to make it relevant to all employees. This will be challenging to do within the project timeline, however, with strategic planning, and discussions with specialists and TD Bank employees it is feasible. The event is only available in-person due to collaborative cybersecurity activities and all event speakers may not sign waivers to share their presentations online. There will be employees who are interested in the event but can't attend because it's in person, however, they can receive information and activities online via email. Overall, there are various challenges to attendee engagement, scope of content, generalized content and the in-person delivery of the event. However, there are effective strategies to address these challenges.

CONCLUSION 13

In conclusion, cybersecurity plays a vital role within the banking sector both for remaining competitive and adhering to government regulations. Cyberattacks are an ever-evolving problem, where attacks are innovating and becoming more invasive. Employees are most vulnerable to cyberattacks and preventable actions must be taken. The increase in cyber incidents from Canadian banks last year has been highly publicized and demonstrates the urgency to address this issue. *Cybersecurity Excellence at TD Bank: Empowering our Employees* is a feasible and effective initiative to foster vigilance of cybersecurity practices and awareness of potential threats to educate employees on the field. By promoting a culture of awareness and vigilance, this seminar marks the beginning of a shift in prioritizing data privacy across the company. The seminar is designed to cater to employees of all levels of experience and backgrounds, as everyone needs to be reminded of company expectations and best practices. Overall, this project demonstrates TD Bank's commitment to cybersecurity and being a trailblazer for innovating cyber practices within the banking sector.