FORTRA

Terranova Security®

Building a Resilient Cyber Security Culture in the Finance Sector

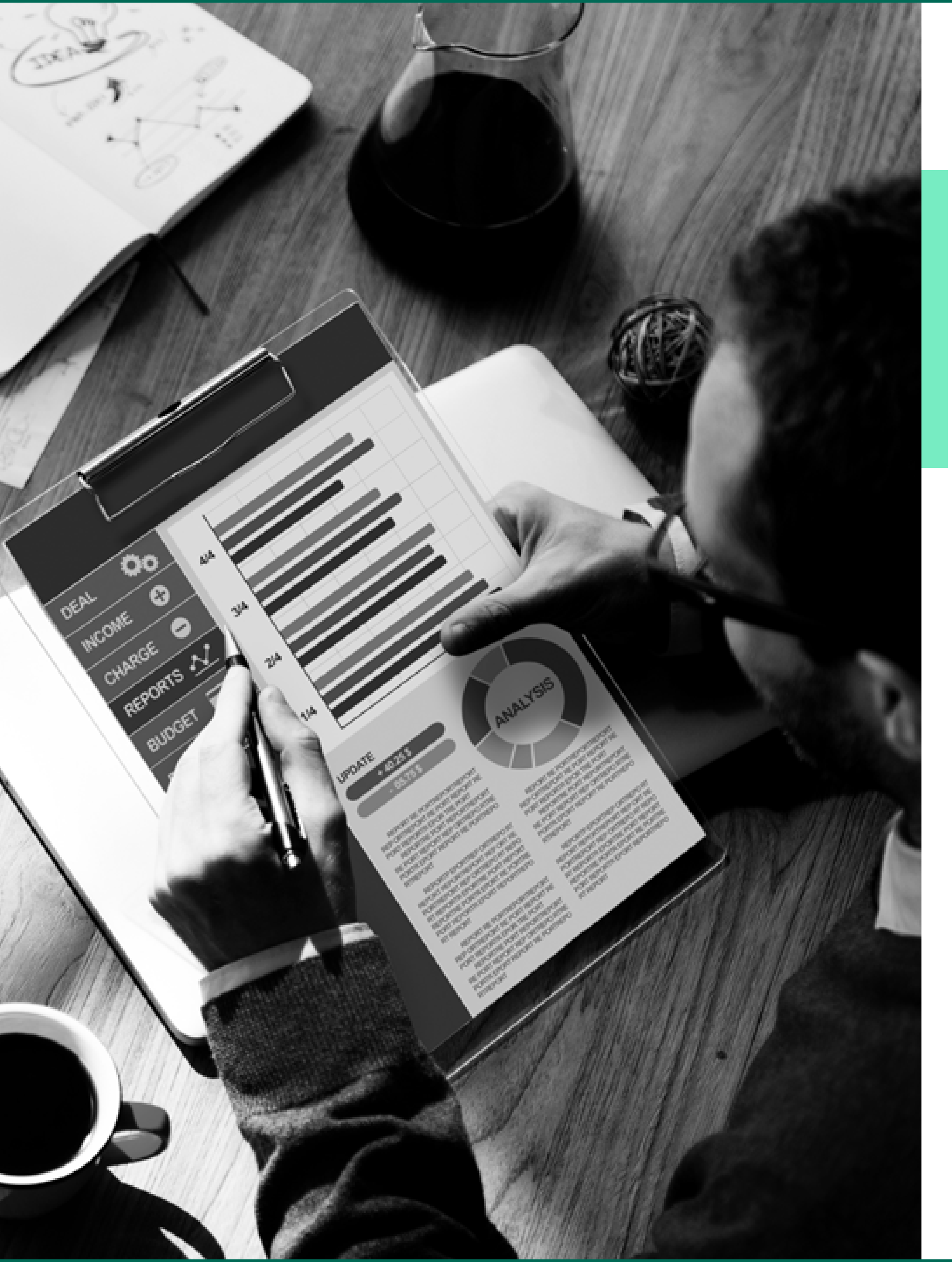
A GUIDE TO OVERCOMING CYBER SECURITY AWARENESS BARRIERS

Introduction

The financial industry has a complex position when it comes to cyber security. Navigating a minefield of regulations and facing an intricate web of interconnected systems, banks and wealth management firms are not just managing money—they're safeguarding the lifeblood of the global economy.

Cyber crime heavily relies on slip-ups and mistakes during system configurations and data transmissions to gain access to sensitive information. According to an IBM study, the average cost of a data breach in the financial industry is $5.90 million, ranking as the second most expensive across all industries.[1]

[1] Source: https://www.ibm.com/reports/data-breach



Cyber attacks in the financial sector often translate directly into financial losses for the affected institutions and financial gains for the cyber criminals. These gains are often used to conduct other criminal activities and further their cyber capabilities. Therefore, the industry's stringent regulatory environment requires strong cyber security measures. However, as cyber criminals continuously advance their tactics—leveraging AI technology—traditional software and physical barriers are no longer sufficient to protect against these evolving threats.

Given that 98% of cyber attacks exploit social engineering tactics targeting employees with access to critical data, it's vital for companies to cultivate a cyber-aware culture, arming their workforce with the knowledge to safeguard against these ever-evolving threats. [2]

This eBook will explain the cyber risks the finance sector faces, address the most common objections related to cyber security investments in this field, and provide tips to build your own cyber security-focused culture.

[2] Source: https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html

CHAPTER 1

Understanding the Risks and Threats to the Finance Sector

Whether it's banking or wealth management, the finance sector is a prime target for hackers because of its direct access to funds and sensitive personal information.

The primary reason is that the finance sector is heavily reliant on technology to maintain its operations and render its services. In addition, the interconnectivity of financial institutions increases the risk, impact, and avenues of cyber attacks, as a breach in one institution can have a cascading effect across the banking network.

Many organizations rely on legacy systems such as mainframes and COBOL programming languages for their backend business applications.

However, organizations that decide to modernize to newer technologies may face additional risks related to cyber security and cloud services.

Luxoft highlights[3] the unique strengths of mainframe security, noting, "Mainframe security is unparalleled. With the potential cyber risks to new platforms and applications, the resilience, transaction management and data safety mainframes provide is vital. Similarly, pervasive encryption and passports offer comprehensive compliance and control for both mobile and resting data."

This conversation around security becomes particularly pertinent for smaller wealth management offices. Often operating without a dedicated IT department, basic security measures may be rushed or glossed over entirely. Given that these organizations frequently use legacy software, these programs sometimes lack the features to protect their users adequately.

Before we can talk about solutions, it's essential to identify the problems. Here are the most common cyber threats faced by the finance industry.

[3] Source: https://www.luxoft.com/blog/why-banks-still-rely-on-cobol-driven-mainframe-systems

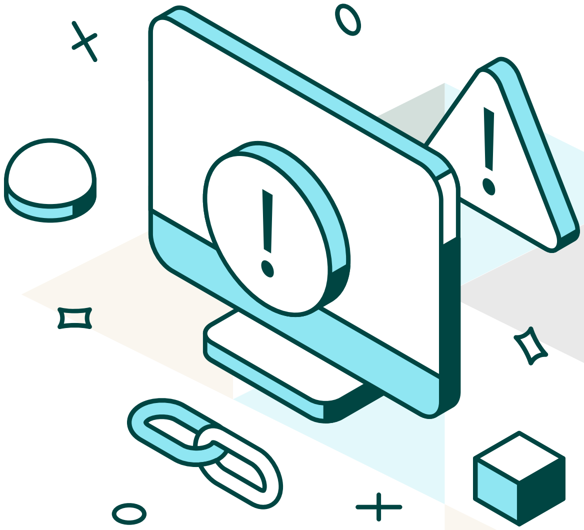
Data and system breaches

A breach can happen through phishing but is often executed via password theft, brute force password guessing attacks, or a vulnerability in a system or application. These attacks become increasingly sophisticated the more critical the safeguarded data is.

A breach in the finance sector can lead to:

- ✓ **Theft of funds**
- ✓ **Opening of fraudulent credit lines**
- ✓ **Identity theft**
- ✓ **Money laundering**
- ✓ **Financing illegal activities**
- ✓ **And many other fraud schemes**

The high value of assets and data combined with the critical role the financial industry plays in the economy makes this sector a high-value target for cyber criminals and organized crime. Breaches represent significant challenges to financial institutions and the agencies put in place to regulate them. Robust security controls, verification procedures, and continuous monitoring are required to prevent such activities.



Ransomware

This form of malware is designed to accomplish a straightforward task: take over a system and lock out all users by encrypting the data until a ransom is paid, usually in cryptocurrency. These kinds of malicious software are challenging to get rid of once allowed to spread on a network, often costing far more than just the price of the ransom.

Banks are a fixture of life for most people worldwide, and their operations cannot stop for any reason. Banks are also trust-based businesses, meaning any blemish to their reputation can severely damage their operations or affect their market value.

This reality makes them ideal targets for ransomware attacks since they are almost always assured to have ample funds readily available and are, therefore, likely to pay the ransom to keep their operations going.

Additionally, with governments and agencies such as the SEC adopting more stringent rules requiring organizations to disclose significant cybersecurity incidents, organizations will have no option but to make these previously hidden events public.[4]

[4] Source: https://www.sec.gov/news/press-release/2023-139

Distributed Denial-of-Service (DDoS) attacks

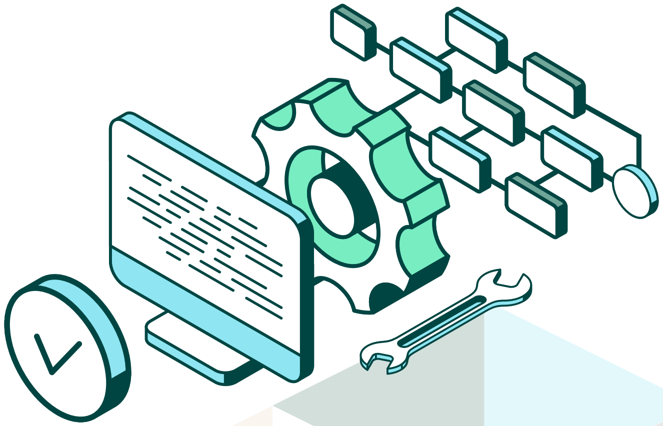
A DDoS attack is executed by sending an overwhelming number of requests to a server every second to overload it, making it unable to process legitimate transactions. While email servers were once a common target of these attacks, with the goal of slowing them down, the trend has shifted.

Nowadays, the predominant methods are ICMP floods or Ping of Death attacks, which overload servers with an excessive number of requests, rather than targeting email systems.

The overwhelmed server or network then shuts down, taking websites and web applications offline.

Over the years, these attacks have fallen out of favor since they are relatively easy to counter with modern servers and solid network architecture. However, if a bank relies on older-generation servers and has slow IT refresh cycles, they can be vulnerable to DDoS attacks.

Banks are also prime targets for hacktivists or nation-states looking to disrupt an institutional service to prove a point or to create economic instability, often the aim of DDoS attacks.



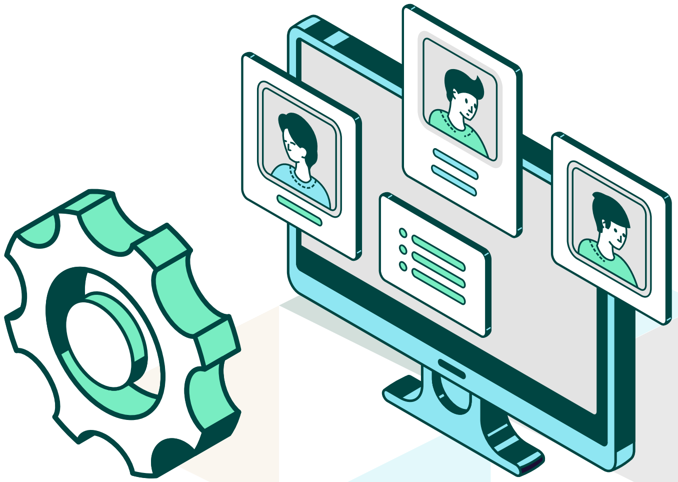
Social engineering

This technique often surfaces as part of a more complex phishing attack centered around harvesting personal information on a specific target to conduct a more personalized attack. The goal is to impersonate a co-worker, supervisor, or business associate convincingly. After gaining the victim's trust, the scammer can then request private company data or convince the victim to transfer funds.

These attacks often occur via email, phone calls, and text messages and may use hacked or spoofed trusted entities to create a fabricated scenario to compromise unsuspecting employees.

Financial institutions are fast-paced environments where sharing multiple sensitive documents and executing numerous large wire transfers are daily realities. This busy setting can lead to a lack of attention, creating the perfect environment for social engineering scams.

Their offices routinely conduct business directly with external individuals, meaning that email domain names can be anything (including Gmail or Hotmail), and spelling mistakes aren't necessarily a good marker of a potential social engineering attempt.

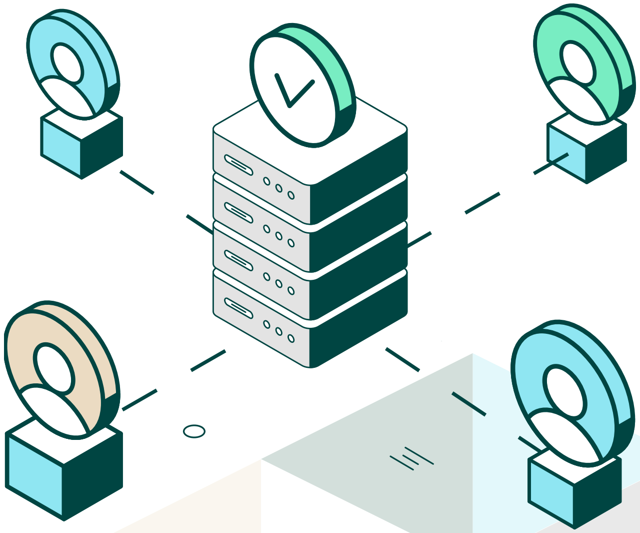


Third-party risks

Banks are often highly distributed entities that operate in several countries and continents. These institutions must then interface with local institutions, suppliers, and other business partners, requiring them to conduct business and establish trust with third parties.

Many also rely on the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system to conduct information transfers and execute banking instructions.

These vendors and partners often have direct API or network access, and a breach at one of these players can spell disaster for the linked bank.

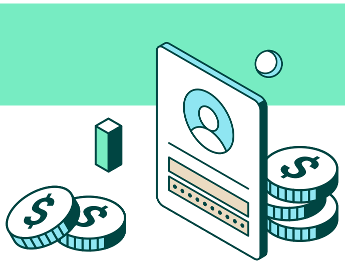


CHAPTER 2

The Impacts of Cyber Risks in Finance

Cyber threats are all relatively common worldwide but can have more damaging impacts specific to the financial industry.

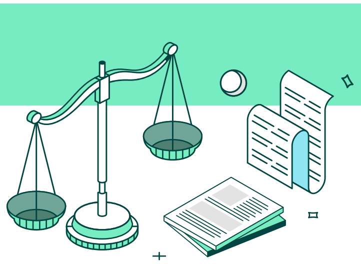
Here are the potential implications of the threats outlined above:



DIRECT FINANCIAL LOSSES

The most obvious target for hackers in the financial industry is client information and funds. When other sectors are targeted, individuals' personal data is often the prize as it allows criminals to gain fraudulent banking access. However, cyber attacks in the financial industry are almost almost always linked to stolen funds, identity theft, or other financial fraud.

These effects may ripple across the economy and cause a broader economic impact. Operational disruptions that affect an institution’s ability to provide its services can affect commerce and other transactions that maintain the economy.



LEGAL AND REGULATORY CONSEQUENCES

The financial industry, governed by stringent regulations such as the Gramm-Leach-Bliley Act (GLBA) in the United States, the Digital Operational Resilience Act (DORA) in the EU and industry standards such as PCI DSS, can face severe consequences that have lasting effects on their business and the market in which they operate.

All these risks and impacts can be significantly mitigated and downright negated by proper cyber security awareness from your users.

Phishing attempts can be prevented entirely by recognizing the warning signs, and most of the other threats become much easier to control if they are spotted and reported early.

REPUTATIONAL DAMAGE

How a bank or financial advisor handles a cyber threat is often more important than the outcome. Did their clients feel safe and informed? Do they think the issue was fixed for the future? Do clients still have trust in their financial institutions?

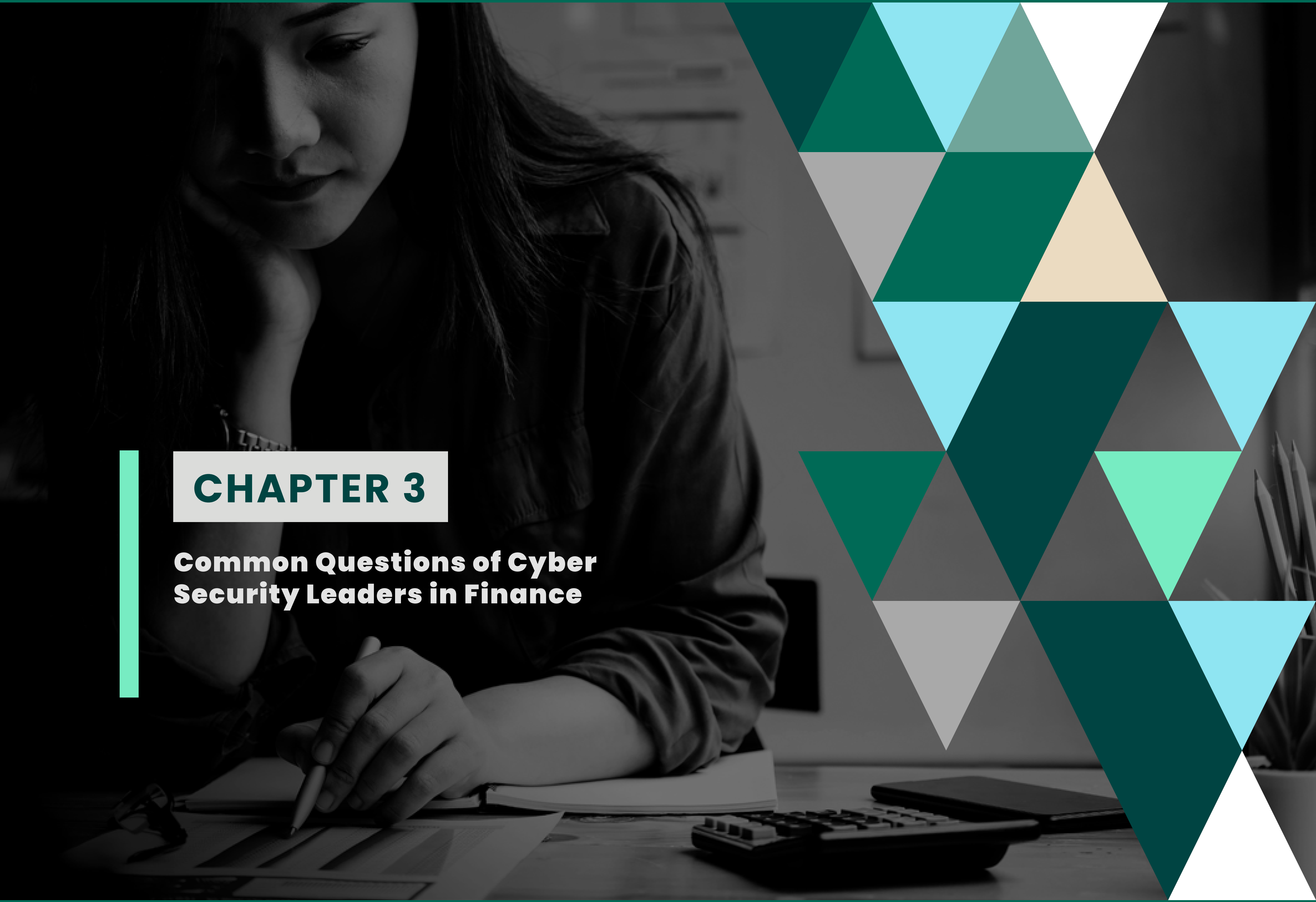
A successful attack, or one that is not properly managed, can cause significant damage to a financial institution’s reputation. Customer trust is a critical component in this sector, and the loss of it can lead to customers changing institutions, which in turn will affect revenues and shareholder value.

Banks can also be targeted without monetary objectives as part of a hacktivism campaign. In these situations, handling the hack is critical, and every second counts. As reported by SCMagazine, DDoS attacks against financial institutions have rapidly increased as a result of the Russia-Ukraine war.[5]

Hacker groups on both sides have been targeting financial institutions they believe to be involved with their rivals, with many small players getting caught in the crossfire. Perhaps the most famous of financial hacktivism cases remains project OpIcarus, launched by Anonymous in 2016, a large-scale call for cyber attacks to "shut down banks."[6] While the project has lost popularity in recent years, the potential of this threat persists.

[5] Source: https://www.scmagazine.com/analysis/report-wartime-hacktivism-is-spilling-over-into-the-financial-services-industry

[6] Source: https://www.reliaquest.com/blog/five-threats-to-financial-services-part-five-hacktivism/



CHAPTER 3

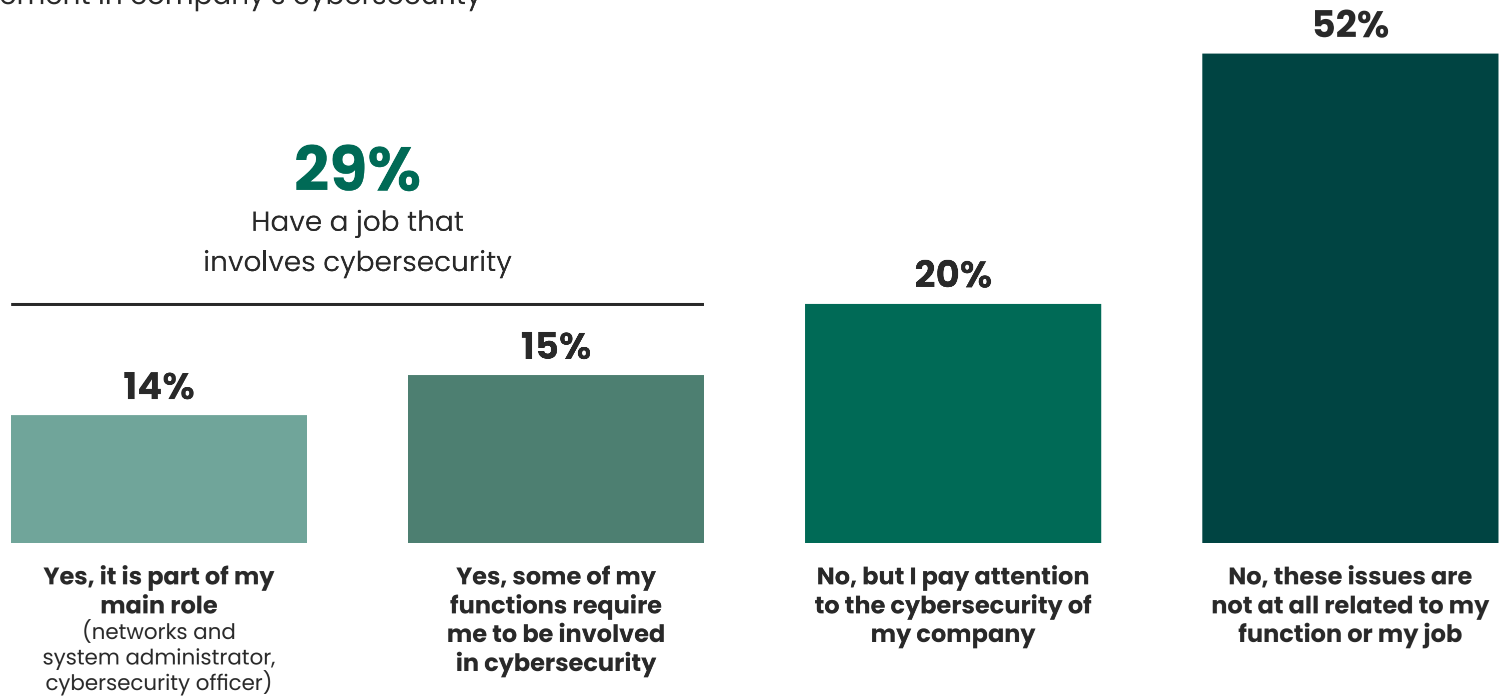
Common Questions of Cyber Security Leaders in Finance

Cyber security can be extremely complex for financial institutions given their numerous endpoints like websites, mobile apps, ATMs, computers in offices and branches, and more.

Additionally, the diverse roles and varying levels of technical expertise among the employees add another layer of complexity to maintaining cyber security. This diversity necessitates solutions that go beyond mere software to effectively safeguard against threats.

52% say their job has nothing to do with cybersecurity

Involvement in company's cybersecurity



In your company, are you involved in IT support in cybersecurity ?

Base=4000: All answering No filters applied

Even though 52% of employees believe their job has nothing to do with protecting organizational data, cyber security isn't just management's concern.[7] The most prominent players in a company's strategy are the employees.

Finance professionals have famously busy schedules, and it's a common issue when trying to allot some of their time to cyber security training. The best way to convince them of the importance of cyber security awareness training is by answering their objections just like you would the leaders.

Below are the most common questions you'll hear from executives as you begin your project of instilling a culture of cyber security awareness.

[7] Source: https://www.terranovasecurity.com/resources/guides/from-data-protection-to-cyber-culture

Question 1: “We already have security measures in place. Why do we need this?”

Banks and wealth management offices almost always have robust cyber security software installed and a complicated server architecture for maximal material protection. However, most outlined threats completely ignore typical software by targeting users directly.

Response: "Most breaches are caused by human error."

Verizon's 2023 Data Breach Investigations Report (DBIR) showed that nearly three out of four breaches (74%) involved a human element.[8] This number underscores that positioning cyber security awareness training as the primary security measure is crucial. It answers threats that no software can reliably counter and is a company's first line of defense on most occasions.

Question 2: “How can we allocate funds for this?”

Even though finance organizations manage a lot of money, they still have strict budgetary rules with much-required approval before deciding.

Response: "Three words: Return on investment."

Cyber security awareness training is the most cost-efficient measure of cyber security and often downright cheaper than any other measure. A company going with this type of initiative will usually be able to save money that can then be reinvested in other employee support programs. In the case of the financial sector, which must comply with cyber security frameworks, cyber security awareness is a mandatory requirement.

[8] Source: https://www.verizon.com/business/resources/reports/dbir/

Question 3: "Didn't our employees already receive training in cyber security awareness?"

This question is common in almost every industry. Prior cyber security training is helpful but must be constantly refreshed and revisited for reliable protection.

Response: "Training is not a one-time event."

Training must be a regular occurrence to be successful. Having a clearly defined schedule around training can often be a selling point to employees. It shows that their workplace cares about their knowledge level and wants to inform them of new threats. Special consideration is also required for new hires and those who switch to a higher-risk role.

Question 4: "Isn't this going to disrupt our work schedule?"

Cyber security awareness training doesn't have to be tedious, long magistral teaching to be effective. Many providers offer bite-sized, quick supplemental training that can be done within the busiest schedules, one day at a time.

Response: "Training saves time and resources."

The alternative to cyber security awareness training is an even more restrictive, hand-holding approach to cyber security: zero-trust architecture. This situation can be costly, tedious to implement, and may offer a worse user experience. Cyber security awareness training is a time-saving measure because it allows for more relaxed physical protections since employees are more knowledgeable about the threats they face and become more confident about the decisions they make. Additionally, data breaches can cost a lot of downtime while your users wait for the systems to go back up—a far less ideal use of everyone's time.

Question 5: “Would hackers even bother with a small target like us?"

A survey by Insurance Business revealed that 60% of small businesses believe they won't be targeted by cyber attackers.[9] However, not being a large target might be an even more significant incentive for cyber criminals, especially compared to what other fields can provide them.

Response: "Small businesses are also at risk."

If you work for a smaller finance organization like a credit union or wealth management office, your employees must understand their role is even more significant. This is especially true for organizations that work with independent agents and brokers, who work on their own devices and home networks but access organizational systems and client data.

Financial companies do so many transactions daily. Every user must recognize the signs of phishing and social engineering.

[9] Source: https://www.insurancebusinessmag.com/ca/news/cyber/small-businesses-underestimating-their-vulnerability-to-cyber-risks--survey-461246.aspx

CHAPTER 4

Reassuring Leaders About the Benefits of Training

When it comes to cyber security awareness training, communicating the right benefits is just as important as the actual content of the training.

Here are some of the most important aspects to lead with when rolling out your cyber security awareness program:

Cost savings

Cyber security awareness training represents not only an affordable upfront investment but also significant potential cost savings from averting data breaches.

Typically, as a response to a cyber incident, organizations tend to invest a significant amount of time and money in cybersecurity defenses as they cannot afford a second incident. This includes purchasing advanced security technologies, hiring staff for forensics analysis, and training staff.

Be transparent about the post-incident costs and how you plan to use the potential savings for new initiatives or programs that benefit employees and the organization. This clarity will help get the company's executives to support this initiative.

Cyber security-aware culture

High levels of cyber security knowledge can become integral to employee culture. Make sure to identify potential cyber security champions that will become the pillars of your program.

When executed correctly, cyber security awareness becomes more than the training, with employees discussing it on their off time and making it an essential part of their day-to-day lives.

The ideal situation is where your employees are not afraid to ask questions, raise their hand if they accidentally did something wrong, and alert someone when they notice an event that may lead to a security incident.

Reputation protection

Many finance sector employees care deeply about their employer's reputation since it's tied to the security of their positions.

These types of training ensure that a breach doesn't tarnish the organization's reputation and competitive position.

This kind of initiative can even become a point of pride for employees, showcasing how cyber security ranks for their company.

CHAPTER 5

Mitigating the Human Risk Factor with Fortra's Terranova Security

Terranova Security's cyber security awareness training solution offers industry-leading courses, phishing simulations, and even first-person game-style modules.

Organizations can change unsafe online behaviors in employees, third-party contractors and suppliers, partners, and other business units. As a result, every stakeholder can consistently detect and avoid common cyber threats.

Engaging, relevant content

Terranova Security offers engaging content to transform unsafe online behaviors into vigilant, threat-detecting practices. High engagement with diverse media leads to better information retention, empowering a proactive defense against cyber threats.

Advanced phishing simulation tool

Terranova Security's advanced phishing simulation tool equips employees to identify and respond to emerging phishing threats effectively. Regular updates and targeted simulations ensure organizations are prepared for real-world cyber attacks.

Gamified content

Terranova Security's gamified training modules make learning about cyber security engaging and competitive, encouraging active participation. This hands-on approach enhances employees' grasp and application of cyber security protocols in their daily roles.

Micro and nano-learning modules

These concise learning modules provide quick, essential cyber security updates to maintain employee vigilance and protocol adherence amidst evolving threats and advanced tactics.

Tailored cyber security training

The adaptability of these programs stands out as a significant advantage. Experts collaborate directly with your organization to create a training plan that addresses your unique requirements and vulnerabilities, ensuring that your staff receives the most effective education, focusing precisely on areas where your organization is most at risk.

How do your phishing click rates stack up against your peers?

The 2023 Gone Phishing Tournament tested the phishing knowledge of 1.3 million end users from organizations of varying sizes in different industries. And we've compiled all our findings in one report.

GET YOUR COPY HERE

Building Cyber Resilience in Finance Through Employee Education

The finance industry has been and will remain a prime target for hackers. Large sums of money and a high potential for societal disruption mean this field gets attacked by financially motivated hackers and hacktivists.

At the scale they're operating and being targeted at, relying on software protections alone would be less than ideal. Almost all the attacks on the finance sector target people over systems, and there is only one way to fix that: advanced employee cyber security knowledge.

Click here to talk to an expert about how Terranova Security's awareness training solution can make a difference for your organization.

BOOK MY DEMO

What Our Clients Have to Say

See how our cyber security solutions have empowered companies just like yours to fortify their defenses and cultivate a security-first culture.

Our case studies showcase real-world success and the transformative impact of our training.

EXPLORE SUCCESS STORIES

FORTRA™

Terranova Security®

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.