mimecast®

Email Security in Finance

Money, Investments & PII Make for a Hacker's Dream Target

section

one.

Financial services — companies, investment firms and fintech — presents a rich pocket for cybercriminals to pick.

Rapid Digital Transformation Leads to Greater Cyber Vulnerability

Money, investments and loads of sensitive personal information are the potential haul for threat actors. Globally, financial services companies have recently seen a major rise in digital transactions, mobile banking and overall email volume, driving them to add more scalable cloud-based systems to their core legacy systems — especially for email. As a result, the potential for cybersecurity breaches has risen. Every new email might be a phishing or malware mule, or a tunnel for ransomware.

In addition to growth in digital communications and transactions, two other factors are expanding the cybersecurity landscape for financial services: new data privacy regulations and the COVID-19 pandemic.

New regulation, starting with the European Union's General Data Protection Regulation (GDPR), South Africa's Protection of Personal Information Act (POPIA), the newly-introduced South African Cybercrimes Bill, and some U.S. state laws, all provide standards for personal data protection that aim to enhance trust and security for digital transactions. And for the UK financial services firms, the Financial Conduct Authority (FCA) is the principal regulator for cyber risks. The FCA's Handbook establishes wide-ranging requirements for firms to manage the risk of cyber breaches, protect their customers, and cooperate with regulators.

But cyberattacks can cause irreparable reputational damage to financial institutions, which rely on customer trust. The COVID-19 pandemic and related social distancing practices caused a hurried (at best) or hasty (at worst) shift to dispersed workforces, opening a plethora of nooks and crannies for cybercriminals to squeeze through, usually via email.

Cybersecurity challenges are not new for financial institutions, but the severity, volume and sophistication of breaches has intensified. Cyberattacks can take a company offline, cause customer panic or shut operations temporarily, all of which lead to financial loss. According to a Ponemon Institute's estimate, the average cost of a data breach in a U.S. financial institution is $5.9 million, which is 52% greater than the average in other sectors.[1]

$5.9 million

is the average cost of a data breach for U.S. financial institutions — 52% higher than other industries.

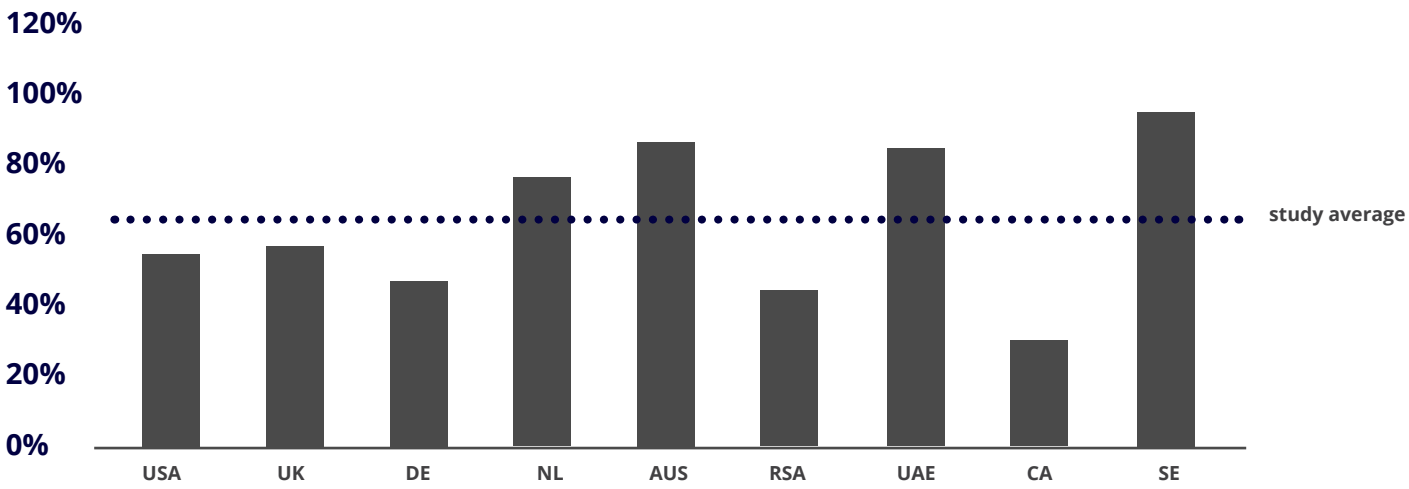
To get an inside perspective on financial institutions' cybersecurity challenges, we surveyed 153 financial services firms as part of Mimecast's State of Email Security 2021 (SOES) report, a global survey of 1,225 information technology and cybersecurity professionals. Among the key findings is that 62% of financial services respondents believe it's likely, extremely likely, or inevitable that their company will experience negative business impact from an email-borne attack during 2021, despite their reputation for being among the best-defended industries.

Concern over the consequences of an email-borne attack was highest among the 25% of respondents who sit in their firms' C-suite (CIO, CTO or CISO). And as the accompanying bar chart of all financial services respondents shows, it was also global.

62%

of financial services respondents believe it's likely, extremely likely, or inevitable that their company will experience negative business impact from an email-borne attack during 2021.

Likely-Inevitable, Experience Negative Business Impact from an Email-Borne Attack by Country



section

two.

Financial Services Firms Are Under Attack

The financial services industry, which includes banks, insurance companies, investment firms and fintech is a perennial target of email attacks. This is due to the nature of dealing with money, the large customer base and the valuable personal data of each customer, such as Social Security numbers or national identification numbers, banking details, contact and income data. The stakes are higher and the potential value of a heist is bigger in financial services. In fact, the cost of data breaches in the financial services industry — including the costs of remediation, recovery and lost business — has ranked among the top three industries for each of the past six years, according to the Ponemon Institute study. [2]

Meanwhile, several trends have fueled digital transaction and email growth, expanding the number of potential financial services attack vectors:

- Financial firms have **embraced online and mobile channels**, which have been widely adopted by their customers.
- COVID-19 has driven more customers to do business in contactless and cashless ways, adding **even more digital volume** to an already valuable target.
- The **number of sensitive emails** between institutions and customers, as well as between employees within institutions, has exploded.

Further, financial services, as an industry, has been technology-challenged as it moved into online and mobile channels. Many institutions had to build out their new digital capabilities on top of legacy systems that have been in place for decades. The resultant hybrid systems create a larger attack surface, which increases the potential for loss.

Email Is the Number One Attack Vector

Businesses communicate with their customers, suppliers, and employees in many ways, but email is king among them. This is even more true in 2021, when workforces are scattered in continuously evolving work-from-home and hybrid in-person situations. Over 25% of finance companies surveyed have 15,000 of more email users, globally — more than any other industry in the SOES report. Further, email volume increased last year in 81% of global finance organizations, according to the study.

With the increases in email volume and reliance comes an increase in email-based threats from cybercriminals. Cyberattacks are rising across all industries and financial services is not immune. In fact, 57% of finance respondents expect the volume of attacks to be among their biggest email security challenges of 2021. Concerns about the volume of attacks was highest in South Africa and UAE.

The sophistication of email attacks is also on the rise, adding a layer of complexity and causing 64% of finance respondents to also name increasingly sophisticated threats among their biggest email security challenges. In regions where fewer respondents expected overall email volume to increase, like Germany and the UK, more respondents believed increased sophistication was their greater concern. However, sophistication of attacks remained of equal or greater concern than the number of attacks even in the two regions where email volume is expected to increase the most — the Netherlands and Sweden.

Attack volume and sophistication rising together is a one-two punch, for sure, leading three of five respondents in financial services (62%) to think their organization could suffer a negative business impact from an email-borne attack in 2021. Their angst is supported by data from the International Monetary Fund that shows cyberattacks, in general, have tripled over the last 10 years and that the financial services industry is most squarely in the crosshairs.[3]

81% **of financial services companies experienced growth in email volume.**

Ransomware and Email Security

Email is the prevalent way that ransomware enters a network, creeping its way around and holding data hostage. And since a network is only as secure as its weakest human link — and financial services companies in our study tend to have more employees — the likelihood of a naïve click on the wrong email link can be high.

It's become a relatively common occurrence that can set off a chain reaction for the victim and their business partners causing:

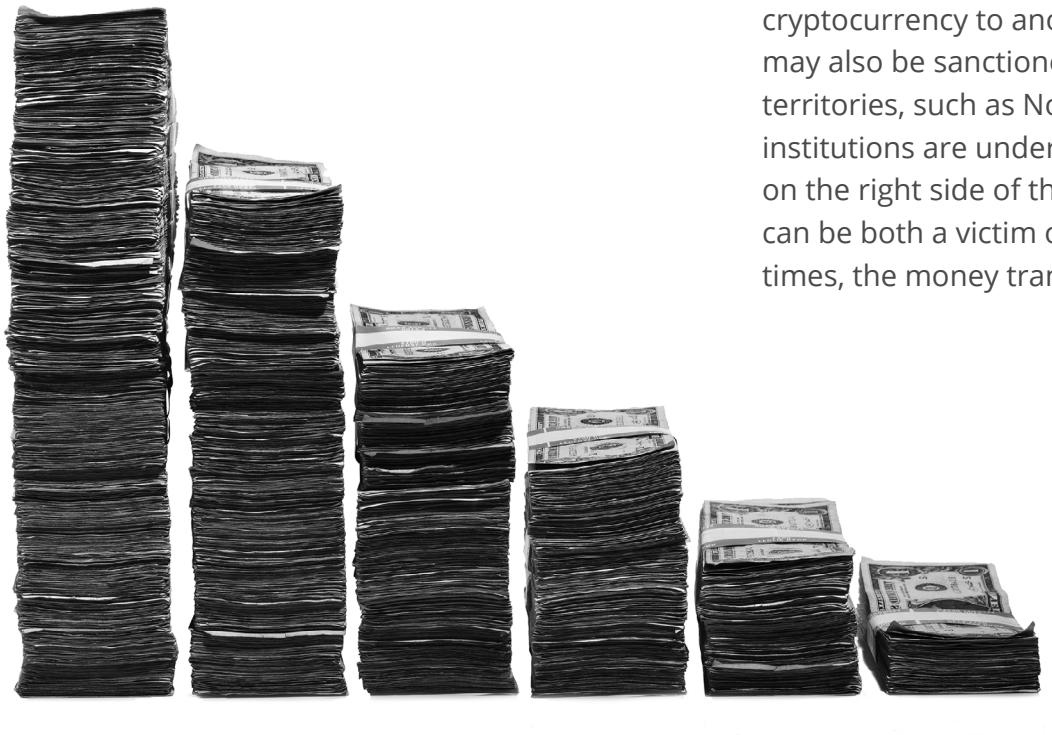
- **increased cost to acquire new customers**
- **reputational losses and reduced goodwill**
- **revenue losses from system downtime**
- **business disruption**
- **lost customers**

The costs of such an attack are staggering, and time is of the essence when they happen. For example, 30% of respondents said their financial firms experienced between 1-4 weeks of operational downtime from a ransomware attack in the past 12 months. Firms of all sizes are faced with the choice of whether or not to pay the ransom. Experts note the growing incidence and sophistication of ransomware attacks has accelerated during the COVID-19 pandemic, likely due to less secure work-from-home environments and increased usage of devices for social connectivity.[4]

53%

of financial services respondents believe it's likely, extremely likely, or inevitable that their company will experience negative business impact from an email-borne attack during 2021.

Ransomware attacks are pervasive within financial services, with more than half (53%) of the surveyed companies indicating that a ransomware attack somewhat or significantly impacted their business within the last 12 months. UAE, Sweden, and Australia lead the pack, with 60-88%, highlighting the global nature of the ransomware challenge.

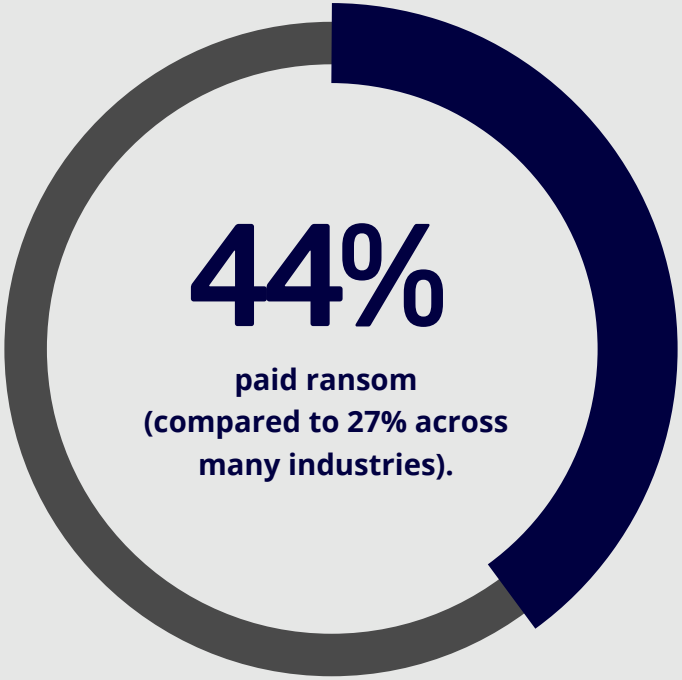


Interestingly, two of those countries also ranked highest in terms of paying ransom, a tactic most law enforcement agencies (such as Europol, the Dutch National Police, and the FBI), advise against.[5] Complicating the issue for financial institutions is that paying ransom may trigger specific anti-money laundering/know your customer (AML/KYC) compliance rules, which exist to ensure account holders can be identified and money trails are clear. These rules are set up to reduce the instance of funding bad actors of any variety. Ransom payments are typically demanded in cryptocurrency to anonymous recipients who may also be sanctioned persons, organizations, or territories, such as North Korea or Iran. Financial institutions are under double the pressure to stay on the right side of the AML laws, because they can be both a victim of ransomware and, at other times, the money transfer agent for another victim.

To pay or not to pay ransom is a challenging squeeze.

Financial services companies may pay more often than other industries: Of finance firms in the SOES report that suffered a ransomware attack in the past 12 months, 44% paid. That compares to 27% across many industries in another global study.[6] Financial services companies may be more apt to succumb to ransomware extortions to avoid the publicity of the security breach and the potential reputation damage it would bring their business.

One study indicates that threats to release stolen data, sometimes referred to as "double extortion," is a feature of 77% of ransomware attacks.[7] But financial services organizations across the world should take careful note of local laws: The South African Cybercrimes Bill, while not yet signed into law, imposes reporting requirements that can carry hefty fines that could add to an organization's reputation damage and business loss.



61%

believe they can recover their data without paying the ransom.

47%

only managed to do so in past attacks.

An interesting gap exists between what the surveyed group believes their financial firm would do if attacked in the future and what actually happened in ransomware attacks during the past 12 months: 61% believe they can recover their data without paying the ransom but only 47% managed to do so in past attacks.

Because it's expected that both ransomware activity and ransom amounts will continue to increase, protecting data with rigorous backup and retention policies are among the best solutions for mitigating permanent loss of data for financial firms.

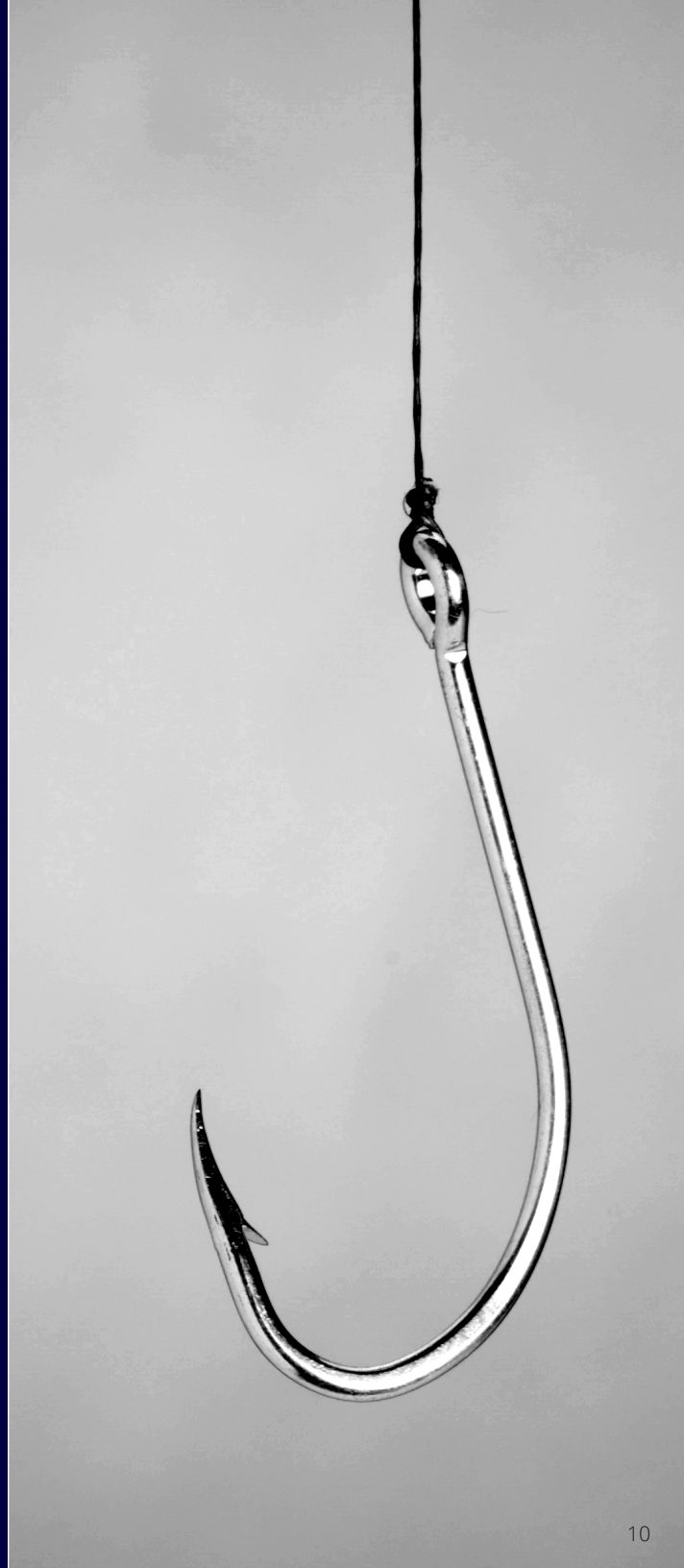
Phishing & Brand Spoofing

Due in large part to the increase in email volume, companies have been abandoning their on-premises solutions and moving their email security to cloud services.[8] It is this sweet spot, where email and cloud accounts intersect, that advanced attacks target.

Within financial services, 60% of SOES respondents saw increases in phishing with malicious links or attachments over the past year (including 24% who said the increases were "large") and 42% noted increases in misuse of their brands via both email and spoofed cloned web domains. In terms of brand misuse, those 42% of respondents included 18% who saw large increases in their brand's misuse in cloned websites and 11% who saw large increases in emails that misappropriated their brands. For a deeper dive into this issue across all industries, see Mimecast's *The State of Brand Protection 2021 report*.

Consistent with the SOES 2021 responses, financial services was the industry most targeted by phishing attacks during Q4 2020.[9] Like all phishing schemes, bad actors cast a wide net hoping to catch a few unsuspecting victims. In this way, they steal passwords, account logins, personal identifiers — all critical info especially for bank accounts, investment accounts or insurance policies.

60% **of financial services companies saw increases in malicious phishing.**



In an already highly regulated industry, various organizations are reevaluating consumer protection regulations, many of which do not currently require financial services companies to reimburse customers who fall victim to phishing, smishing or vishing (via email, text or telephone, respectively). However, the four largest UK banks have signed a voluntary code of practice, the Contingent Reimbursement Model (CRM) Code, that does just that, increasing the cost of scams that exploit these financial institutions' brands.

In scams involving spoofed or cloned web domains, a copy of the financial institution's website is built to look like the original and is filled with malicious links. The links aim to dupe users into entering confidential information through a deceptively real looking login portal, or to download malware onto their device. This is a real problem in financial services companies for both marketers who are building and promoting a trustworthy brand and for security teams who are tasked with customer authentication. One regional bank CISO stated that his bank experiences 10 or 11 such attacks each month via his bank's websites, fraudulent mobile apps, or social media accounts. Left unchecked, these will "pollute your brand," he said, adding that IT security and marketing should work together to protect their brand. One way they do this is by monitoring domain name registrations.

Malicious links aim to dupe users into entering confidential information through a deceptively real-looking login portal, or to download malware onto their device.

10 or 11

such attacks each month via websites, fraudulent mobile apps, or social media accounts.

section

three.

Can Financial Services Companies be More Cyber Resilient?

As an industry, many financial firms already have active cyber resilience plans, so the challenge is to continually evolve them to keep pace with the advancing sophistication of attacks. Additionally, they will need to stay ahead of changing regulations. Their cyber resilience plans will likely require layering cloud email, reevaluating distributed workforce technology and enhancing their security culture.

Layering Cloud Email

Banks, insurance companies and investment firms have adopted cloud-based email systems — most notably, Microsoft 365 — to help manage the vast increases in email volume that comes along with the increases in digital transactions and dispersed workforces.

However, along with the benefits that cloud-based email solutions bring, including cost-effectiveness, quick implementation time, expanded access and scalability, there exists an embedded security challenge: the "single-lock" monoculture. If Microsoft 365 provides an institution's only form of email security, once a bad actor gets past it, they're in.

Three factors exacerbate this security monoculture challenge:

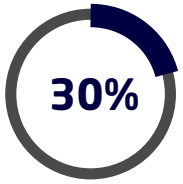
Microsoft's dominance makes it the prime target on which cyberattackers focus

Cyberattackers themselves often use Microsoft services from which to launch attacks, making them appear more legitimate

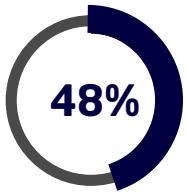
Less than 25% of financial services SOES respondents believe that Microsoft 365 provides world class email security

As a result, financial services companies are opting to layer in additional security software.

In fact, 30% already have a second layer in place and another 48% have plans to put one in place. In doing so, financial institutions can better meet the security expectations of their customers and the requirements of their regulators.



already have a second layer in place.



have plans to put a second layer in place.

Getting Back to Basics: Training to Instill Good Security Hygiene

One of the ways financial services companies can combat the rising threat of email-borne cyberattacks is to double down on building a strong security culture among employees. Reviewing technology and focusing on staff security awareness training are two ways to achieve this goal.

The pace of pandemic shutdowns caused businesses to quickly move to dispersed work environments, often requiring innovative tactics that sacrificed cybersecurity hygiene out of necessity. For example, some IT departments hastily purchased laptops at retail for employees, trading off configuration and security standards in return for availability, to keep businesses running.

And then these sub-standard laptops are hooked into networks using vulnerable remote access connections. All of this raised the susceptibility to attack. Moving forward, security teams will need to review these "temporary" solutions and bring those expected to persist up to snuff.

With this backdrop, it's understandable that 72% of financial services respondents believe there is an elevated level of risk that employees can make a serious security mistake with their personal email. Poor password hygiene is also a concern among 71% of finance respondents.

72% believe there is an elevated level of risk that employees can make a serious security mistake with their personal email. Poor password hygiene is also a concern among 71% of finance respondents.

The other part of the effort includes training employees to increase their awareness of cybersecurity issues. These training programs, which aim to heighten security awareness and change behavior, are a high-priority tactic among two-thirds of IT professionals in companies with more than 100 people, according to a recent Forrester study.[10] Interestingly, financial services companies do not stand out in this regard despite being a highly targeted sector.

Only 44% of financial companies provide security awareness training on a monthly basis or greater frequency, compared with 46% of companies across all industries. The largest concentration of finance companies — 37% — provide only quarterly training.

In terms of security training methods, financial services industry results are a mixed bag, with three methods leading the average for all industries and three lagging (see Figure). The industry is better than most when it comes to automated tactics, including online tests, interactive videos, and interstitial prompting. However, it is behind the curve when it comes to group and one-on-one training and printed reference collateral.

37% **of financial services companies provide employees with security awareness training only quarterly.**

	Total		Financial Services	
Total	**1225**	**100%**	**153**	**100%**
Group training sessions with our IT or IT security team	700	57%	77	50%
A formal online test to learn about threats and prompts questions to respond to	574	47%	79	52%
An emailed or printed list of tips to keep in mind	525	43%	64	42%
Interactive videos highlighting best/ worst practices to keep in mind	523	43%	79	52%
One-on-one training sessions with our IT or IT security team	498	41%	79	52%
Sends prompts for me to note whether a link is “safe” prior to allowing me to visit certain websites	463	38%	67	44%
Other	4	0%	1	1%
My company doesn’t provide any training	15	1%	1	1%

Preparing for Cyber Resilience Makes a Real Difference

In cybersecurity, as with most things in life, being prepared can make all the difference. The good news is that financial services organizations are better prepared than most: 53% of finance firms surveyed have a cyber resilience strategy already in place, compared with only 44% of all SOES 2021 respondents. That means they are better prepared to respond to and recover from cyberattacks.

53%

of financial services companies without a cyber resilience plan expect to roll one out within the next year.

How much better? Thirty percent of finance firms WITH a cyber resilience strategy in place reported experiencing none of the following negative consequences of a cyberattack, compared with only 11% of firms WITHOUT a cyber resilience strategy in place. In other words, nearly nine out of 10 financial services companies (89%) without a cyber resilience strategy experienced one or more of:

- **business distruption**
- **data loss**
- **financial loss/lost money**
- **reputation damage**
- **impacts to regulatory compliance**
- **impact to employee productivity**

Likewise, certain industries that make greater use of collaboration tools exhibit higher anxiety over their safety. These include the construction, energy, consumer services and business services sectors, where the level of concern ranged from 76% (construction) to 86% (business and professional services) of respondents.

Even worse, some companies without a cyber resilience strategy experienced two or more of the effects listed — and one firm reported suffering all six.

Luckily, another 39% of financial services respondents that don't have a cyber resilience strategy in place are planning to roll one out within the next year, which would lift to 92% the finance firms with a resilience strategy (compared to 90% for all respondents). Likewise, the Mimecast study also found that finance firms are ahead of the study average in terms of already using email filtering for inbound, outbound and internal emails.

39% **of financial services companies without a cyber resilience plan expect to roll one out within the next year.**

Key Takeaways

Because digital/mobile financial services activity is expected to continue its rapid rise, so is the rate and sophistication of cyberattacks on finance firms and their customers. Further, cybercriminals will continue to exploit the fallout of COVID-19 and firms' dispersed workforces. The way forward to a more secure future for financial services firms includes these five key approaches:

.01 Build multilayered defenses.

Since email remains the most common threat vector and its volume is expected to increase, financial firms need to layer multiple security technologies to protect their email systems. A multilayered defense provides the best chance to neutralize this expanding threat.

.02 Reassess technology put in place during the pandemic.

For cybercriminals, email remains the most common method for carrying out their incursions, and phishing in particular has become much more pernicious since the pandemic began. To defeat the growing sophistication of these attacks, multiple technologies need to be employed. Such multilayered defenses complement and backstop one another; if a given attack sidesteps one defense, there are others in place that can neutralize the threat.

.03 Pay ransomware special attention.

The threat of ransomware, its potential costs and its AML complexities all continue to increase. While most of these attacks are email-borne and layered defenses can help, protecting data with rigorous backup and retention policies — that include off-network repositories — are important solutions for mitigating permanent loss of data for financial firms. Preserving customer trust and reputation are critical to a financial firm's business success.

.04 Enhance security awareness training.

The biggest potential difference can be made shoring up cybersecurity's weakest links: the people. Financial firms need to extend their leading security awareness training practices with more personalized/individualized training and greater frequency.

.05 Accelerate cyber resilience strategy development.

Financial services companies appear to grasp cyber preparedness better than most. However, not all firms are there yet. Those that don't yet have their resilience strategies in place should accelerate their development. And for those that do, the importance of sustained vigilance, updating and maintaining their cyber resilience strategies cannot be overstated.

mimecast®

Relentless protection. Resilient world.™

1. Cost of a Data Breach, Ponemon Institute and IBM
2. Ibid.
3. "Cyber Risk is the New Threat to Financial Stability," IMF Blog
4. "Ransomware is growing at an alarming rate, warns GCHQ chief," ZDNet
5. Combatting Ransomware, Institute for Security and Technology
6. Global Security Attitude Survey, Crowdstrike
7. "Ransomware Attacks a Growing Global Security and Financial Threat," FitchRatings
8. "Cloud-based Email Security Market- Growth, Trends, Covid-19 and Forecasts (2021-2026)," Mordor Intelligence
9. "Online Industries Most Targeted by Phishing Attacks as of the 4th Quarter 2020," Statista
10. "Don't Just Educate: Create Cybersafe Behavior," Forrester

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.

GL-3271