**GUIDE** *(Cybersecurity)*

# Cybersecurity Challenges in Financial Services – Market Survey Report

A cyber-attack on the financial sector has the potential to cause substantial damage. This was all-too-clear in August, when the New Zealand stock exchange was knocked offline two days in a row by a distributed denial of service (DDoS) cyber-attack thought to have originated from abroad.

Amid challenging Covid-19 conditions and accelerating digital transformation initiatives, the supply chain is one of the most common avenues for attack. Take, for example, the infamous 2017 Equifax breach which saw hackers expose details including social security numbers after the company failed to patch a server.

This successful attack did not just impact Equifax: its supply chain including both Visa and MasterCard sent alerts to banks notifying them that 200,000 credit cards could have also been compromised.

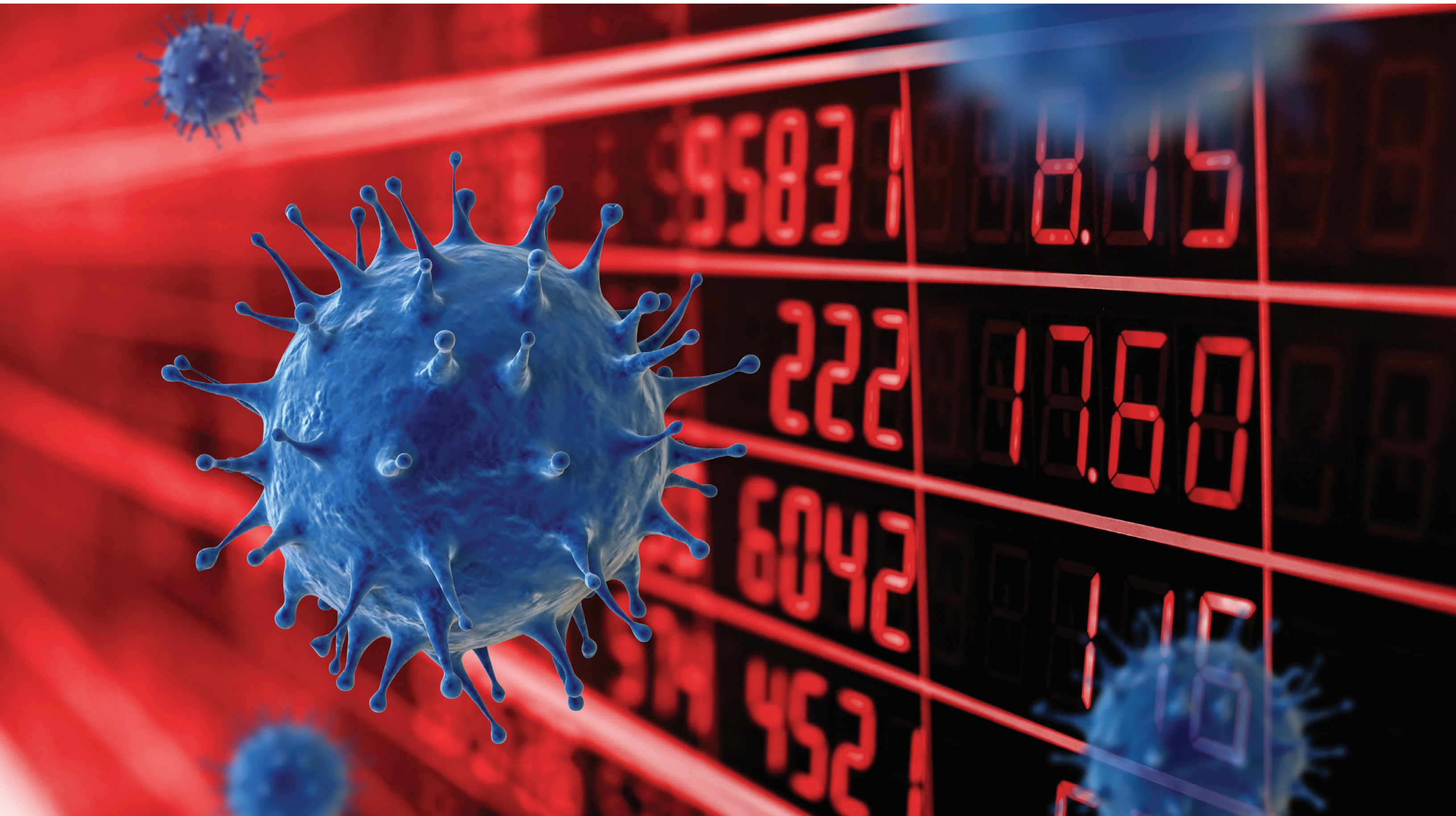
Another supply chain based hack was the 2018 British Airways breach, which saw attackers steal customer payment details through malicious code planted in third party software on the airline's site. A similar attack had hit events firm Ticketmaster during the same year, with both breaches thought to have been perpetrated by the Magecart group, which targets e-commerce businesses.

In addition to supply chain risk, the financial sector faces strict regulation over data privacy and security, complicating things further. Banks must comply with regulation such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Update to Data Protection Regulation (GDPR) in increasingly challenging Covid-19 conditions.

This is all set against a backdrop of a surge in cyber-attacks on financial services businesses. Nearly two thirds (65%) of large financial organizations have suffered a cyber-attack in the last 12 months, according to data security provider HelpSystems' survey of 250 CISO/CIOs across the globe.

Since Covid-19 hit this year, the risk has elevated further, with 45% seeing increased cybersecurity attacks during this period. The threats span multiple vectors as remote working becomes the norm across the financial services industry.

As financial CISO/CIOs consider the next three years amid Covid-19 uncertainty, it creates a huge cybersecurity challenge: How can financial organizations embrace digital transformation and enable efficient working from home as cybersecurity threats surge?



## Strategic Challenges

Financial firms face a plethora of cybersecurity and data protection challenges. This has been exacerbated during Covid-19, when organizations are dealing with an acceleration towards digital transformation while managing a remote workforce.

Financial businesses already know and fear the impact of a cyber-attack. When asked which implications of a cybersecurity attack or breach they fear the most, 51% say damage to brand reputation. Meanwhile, 43% are afraid of sensitive customer data being breached, 40% are concerned about customer-facing downtime, and 34% cite disruption to internal operations as an issue.

The threats are vast, but the most concerning challenge that could cause the most damage in the next 12 months is the potential for cybersecurity weakness in the supply chain, according to nearly half (46%) of CISO/CIOs surveyed.

This is closely followed by increased working from home during Covid-19, selected by 36% of respondents as the threat with the potential to cause the most damage in the next 12 months.

Meanwhile, 35% cite hackers gaining access to core systems as the most damaging and another 35% say insider threat, whether malicious or accidental, has the potential to cause havoc. Data breaches (31%), ransomware attacks (28%) and nation-state cyber-attacks and espionage (24%) are also highly cited.

In three years' time, the main cybersecurity challenge for financial firms is digital transformation, say 41% of those surveyed. Linking to this, the transition to remote working beyond the current climate is called out by 28% of respondents.

Amid this complex environment, it's no surprise that 92% of financial sector organizations have increased their cybersecurity spend over the previous 12 months – 26% significantly so. "It's a highly challenging cybersecurity landscape for the financial services sector, with many CISO/CIOs focused on battling day-to-day threats while trying to achieve broader strategic objectives," says Kate Bolseth, CEO, HelpSystems. "Technology is a key part of cybersecurity of course, and no organization will ever be secure without the right security solutions to protect the organization here and now. But of equal importance, especially for longer-term strategic goals, is ensuring the right processes are in place and educating and training employees."

## Supply Chain Attacks and How to Protect Against Them

It's been established that managing supply chain risk is one of the biggest single issues for financial firms. At a time of increasing digital transformation leading to a more digital supply chain, any organization is only as strong as its weakest link.

Cyber-criminals know this, and often look for weaknesses in a third-party supplier to leapfrog into their intended victim's systems. Whether a complex breach, such as the Lockheed Martin data hack of RSA tokens, or a simpler attack caused by 'trusted' employees accessing information they shouldn't, the whole supply chain is at risk and its security must be taken seriously.

"There are many case studies that demonstrate the vulnerability of supply chains to compromise," says Stewart Room, Global Head of Data Protection and Cyber Security at DWF. He cites the example of the Magecart hack — an attack that sees malicious code injected into sites to steal payment details. This has highlighted the vulnerability of payment services to supply chain cybersecurity weakness, he says.

***" The pandemic only adds to the focus, because it has required many operational adjustments, which naturally involve changes to the supply chain and the attack surface that it represents."***

Mitigation is often as simple as asking suppliers about their cybersecurity policies to ensure they are robust. Transparency is key, including better due diligence on third-party relationships.

## Regulatory Challenges

The financial services sector is one of the most highly regulated in the economy. In the UK, financial organizations have to comply with the GDPR/UK Data Protection Act, PCI DSS as well as non-sector specific regulations covering critical infrastructure.

These regulations require organizations to put in place appropriate measures for data management, including for the purposes of security. "Failure to do so entails many legal risks, with reputational consequences," says Room.

Almost one third of organizations surveyed say regulatory fines as a consequence of poor security are a concern. While it's a good idea that organizations keep a close eye on regulatory risk, Room says it would be a mistake to ignore litigation.

"Litigation following a security breach is a growing risk in many parts of the world, especially where the breach impacts consumers or business-to-business relationships. The UK is one of the countries where litigation risk truly stands out right now, but momentum is growing in other countries too."

Meanwhile, half of financial CISO/CIOs say data visibility is a challenge – a major concern given that this is an integral factor in regulatory compliance. "The GDPR, which triggered countless data transformation programmes between 2016 and 2018, put the need for data visibility on an express legislative footing," Room says. "European data protection regulators will find this statistic alarming."

It is therefore vital that financial firms get a handle on the data they have, where it resides, and how it travels for data visibility, using the right tools and processes. With better understanding and more control, it's easier to meet regulatory challenges, Room says.

## Future Challenges

In a complex attack landscape exacerbated by Covid-19, it's clear that people, processes and technology are key. During Covid-19 as the insider threat is elevated with people working from home, secure file transfer is cited as a key investment priority for two-thirds (64%) of CISO/CIOs. It's an urgent issue that needs to be resolved, but training on its own is not enough and can be a challenge: Internal cybersecurity fatigue is cited by 28% as an issue for financial CISO/CIOs.

Fatigue is a problem party because employees are struggling under the pressure of being constantly trained, especially when they are communicating over video, and security is often a barrier to their day to day jobs.

Technology can help alleviate the pressure by, for example, allowing more automation within the business. It's true to say humans will always make errors no matter how much training they have, and it's a good idea to take some of this responsibility — and risk — away.

At the same time, the survey found that a quarter of financial CISO/CIOs are concerned with having too many manual processes in their business. This has been elevated during Covid-19, CISO/CIOs say, and there is now an increased need for automation in to free up IT staff from manual tasks.

Another concern is outdated IT infrastructure (37%). This is a particular concern because it shows just how many firms have not learnt from the WannaCry attack that ravaged the NHS, taking advantage of outdated Windows systems.

Adding to this, a complex environment is not helping financial firms. 78% believe their organization is using too many cybersecurity tools, while 65% say that these do not integrate well with other tools. At the same time, 84% say too many cybersecurity tools make their organization's security environment unwieldy to manage and reduce its effectiveness.

Getting the right technology in place to support people and processes is integral. When selecting a vendor, it's important to seek value for money while ensuring that tools work effectively and integrate well together.

Securing financial services isn't easy. In extremely challenging conditions exacerbated by Covid-19, there's no one change that can ensure security. Overall, it's important to be flexible while taking a risk-based approach.

Bolseth outlines the challenge: "Organizations need to make the transition to digital, meet regulatory demands, secure a remote workforce in the light of Covid-19 and protect the organization against day-to-day threats such as ransomware. There's no silver bullet, just constant evolution in the face of the changing threatscape."

## Conclusion

The financial sector is under pressure and this is only increasing during Covid-19. There are multiple challenges but perhaps the biggest issue in the coming three years will be digital transformation. The area has been accelerated during Covid-19 and is the backdrop for an elevated supply chain risk.

To address these challenges, it boils down to a combination of people, processes, and technology. Room advises a holistic approach to security taking into account shadow IT concerns prompted by the acceleration of digital transformation due to Covid-19, the regulatory environment and supply chain risk.

Education and training is key, but simply educating users on how to recognize and report a suspicious email is not enough on its own. "It only takes one person to accidentally open a document or click on a URL for malware to gain entry," Bolseth says. "For the next defense layer, organizations need to augment their email security technology to remove infected files and neutralize URLs before they reach peoples' inboxes."

As financial firms grapple with complex security problems under continuing pressure to innovate, the most important aspect is planning. "From a risk management perspective, transformation exercises always present challenges to security, due to the pace, extent and focus of change," says Bolseth. "Where transformation encompasses all of these features, the risks will be elevated, so proper planning is key."

## Covid-19 Challenges in the Financial Sector

Covid-19 has put pressure on all industries, not least the highly regulated, increasingly digital financial sector. It's therefore no surprise that Covid-19 has had an impact on nearly all financial firms' strategy.

Almost half of respondents feel that Covid-19 has accelerated digital transformation-related changes already in discussions, such as a move to Office365.

According to the survey, 42% of financial sector firms say securing the remote workforce has become a main cybersecurity objective, while 47% have increased spend on secure collaboration tools.

The swift move to home working has also seen employees emailing and sharing documents from home devices more than ever. This raises a number of cybersecurity questions which is why the past few months have seen secure file transfer solutions emerge as a key technology, according to 64% of those surveyed.

Sharing files outside of an organization can leave it vulnerable to data loss and ransomware, with cyber-criminals quick to pounce on any weaknesses in the system.

There are many solutions to address this, but many of them block the collaboration at source. While this is secure, it is also highly restrictive to day-to-day operations. Waiting for an important file to arrive is frustrating and can lead to missed deadlines and opportunities.

During Covid-19 and beyond, it's important that firms address this, allowing employees to collaborate while remaining as secure as possible.

# COVID-19 RELATED CYBERSECURITY CHALLENGES IN FINANCIAL SERVICES

We asked CISO/CIOs working in large financial service organizations across the world about the impact the current pandemic has had on their cybersecurity strategies.

| | |
|---|---|
| 50% | It has increased the need for automation to free up IT staff from manual tasks |
| 49% | It has accelerated changes that were already in discussion, such as a move to Microsoft 365 |
| 47% | We have increased investment in secure collaboration tools |
| 46% | We had to re-evaluate our cybersecurity training and policies to better reflect the increased home working |
| 45% | We have noticed more cybersecurity incidents since the increase in home working |
| 45% | We have had to provide more cybersecurity with the same budget, technology, and resources |
| 44% | Securing the remote workforce has become a main cybersecurity objective |
| 36% | Our existing cybersecurity tools were not capable of adapting to the change in working patterns |
| 35% | We have updated our regulatory best practices |

## About the Research

This research was conducted by technology research firm, Vanson Bourne, on behalf of Clearswift in August and September 2020. A total of 250 senior cybersecurity and IT decision-makers (209 CISOs, 41 CIOs) in large global FS organizations were polled – 50 each in the US, UK, The Netherlands, Germany, and Australia .

## REFERENCES:

Equifax Hack: Keep Your Friends Close, but Your Supply Chain Closer
https://www.securityweek.com/equifax-hack-keep-your-friends-close-your-supply-chain-closer

British Airways breach: How did hackers get in?
https://www.bbc.co.uk/news/technology-45446529

New Zealand stock exchange halted by cyber-attack
https://www.bbc.co.uk/news/53918580

Magecart: Group behind BA and Ticketmaster breaches is targeting hundreds of sites
https://tech.newstatesman.com/security/magecart-ba-ticketmaster

PCI Security Standards Council
https://www.pcisecuritystandards.org/pci_security/

Stolen data is tracked to hacking at Lockheed
https://www.nytimes.com/2011/06/04/technology/04security.html

5 cybersecurity threats you didn't know you should be threatened by
https://www.clearswift.com/blog/2019/10/21/5-cyber-security-threats-you-didn%E2%80%99t-know-you-should-be-threatened

5 ways to tighten cybersecurity working from home
https://www.goanywhere.com/blog/5-ways-to-tighten-cybersecurity-working-from-home

How to protect your organization from advanced persistent threats
https://www.clearswift.com/blog/2020/09/03/how-protect-your-organization-advanced-persistent-threats

File transfer solutions emerge as key technology for the age of collaboration
https://www.clearswift.com/blog/2020/06/18/file-transfer-solutions-emerge-key-technology-age-collaboration

ICO guide to GDPR
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

helpsystems

www.helpsystems.com

**About HelpSystems**

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.