NOT IF BUT WHEN:

How to Build Cyber-Resilience in Financial Services Organisations

A SPECIAL REPORT BY SAYER HAWORTH RESEARCH & INSIGHTS

On 26 February this year, we invited senior executives and Board members from SME Financial Services companies to an exclusive briefing by cybersecurity experts Robert Hannigan and Tom Moore, from the specialist consultancy BlueVoyant.

Drawing from those conversations, supplemented by our own research, this report investigates the evolving cybercrime business ecosystem and highlights some of the key vulnerabilities of financial services organisations. We also explore incident response strategies that can help to minimise the resulting damage – both monetary and regulatory.

SAYER HAWORTH

One-Minute Read

The “Nation of Cybercrime” is now equivalent to the world’s third biggest economy, after the United States and China. Geopolitical instability is leading to nation states becoming more active in ransomware and other attacks – both directly and through criminal proxies.

Supply chains are the critical weak point being exploited by threat actors, accounting for some 80% of cybercrime incidents. As a result, it is imperative that supply chain collaboration is built into commercial contracts – including retroactively if possible.

Recent and upcoming legislation, including the EU’s NIS2 Directive and Digital Operational Resilience Act (DORA), plus the UK’s Cyber Security and Resilience Bill, is amplifying the regulatory risk of cyber attacks on financial services institutions.

Developing organisational ‘muscle memory’ through regular incident response exercising is key to reducing the severity of the eventual outcome. Ownership resides at Board/ExCo level – cybersecurity must therefore be considered a leadership discipline, not merely the preserve of technology specialists.

Exective Summary

The Scale of the Problem

Cybercrime is becoming more organised and professional, driven by both commercial and geopolitical imperatives. A BlueVoyant survey found that 94% of respondents had experienced a malware, ransomware or social engineering (phishing) event in H2, 2025. Criminal ecosystems now mirror legitimate supply chains, delivering pre-packaged 'Ransomware as a Service' that is drastically reducing the barriers to entry.

How Secure is your Supply Chain?

A company's supply chain has become the most prominent target for cyber attacks by an overwhelming margin, accounting for some 80% of incidents according to BlueVoyant. Organisations must therefore manage not just their own cyber threat environment, but also ensure visibility, monitoring and protection of all third-party relationships that might offer gateways to cybercriminals.

The Increasing Regulatory Risk from Data Breaches

Cybercriminals are exploiting the growing impact of reputational and regulatory damage from data breaches. As such, a capacity to deal swiftly, openly and professionally with regulators must form an essential element of any incident response plan. This is especially true in financial services, which is already among the most heavily regulated business sectors, with future legislation such as the UK's Cyber Security and Resilience Bill likely to add further demands.

Cyber-Resilience is a Leadership Function, not Just a Technology Function

The ability to recover quickly from a ransomware or other cyber attack can be largely attributed to having a well-rehearsed, usable, practical and fit-for-purpose incident response plan. Board/ExCo members must regard cybersecurity as another key risk factor, alongside financial, operational, health & safety and other risks. All these demands are influencing the skills and attributes required in the C-suite.

AI as a Tool for Attackers and Defenders

For cyber threat actors, artificial intelligence (AI) offers the capacity to supercharge existing attack strategies by enabling them to identify and exploit vulnerabilities much more quickly and with greater agility than previously possible. On the defensive side, the technology's ability to refactor code means it can be deployed to locate and rectify weaknesses in system designs and/or networks.

> **"Supply chain attacks now account for around 80% of cyber incidents."**

Introduction

Understanding the Scale of the Problem

Although commercial confidentialities mean an exact figure for global cybercrime proceeds is impossible to calculate, few would dispute the World Economic Forum's estimation that a 'Nation of Cybercriminals' would rank behind only the United States and China in terms of its economic output. Ransomware alone is projected to cost governments and businesses $74 billion in 2026, according to calculations by *Cybercrime Magazine*.

The problem is widespread: some 94% of firms surveyed by BlueVoyant reported some kind of malware, ransomware or social engineering (phishing) event in the second half of 2025. In addition, the company has seen a near 200% increase in social engineering attacks year-on-year. It genuinely is a case of 'not if, but when'.

Two major factors are driving the current surge in cybercrime: one commercial, one political.

Breaking Down the Barriers to Entry

As with legitimate business sectors, today's cybercriminals are benefiting from enhanced technology and a 'professional services' ecosystem capable of providing fast, comprehensive and relatively inexpensive support.

In this era of 'Ransomware as a Service', a cybercrime threat actor no longer needs to commit time and resources to developing bespoke software tools; they can simply purchase these 'off the shelf' via the dark web or peer-to-peer sharing sites, paying a portion (usually around 30%) of any money extorted back to the license holder.

Through the same channels, cybercriminals can also acquire lists of target companies with identified vulnerabilities from so-called 'initial access brokers' – a direct analogue of the qualified leads used by legitimate businesses.

All of this means that the barriers to entry for would-be cybercriminals are at their lowest ever levels, while the advent of these specialised services has increased the speed, scale and effectiveness of cyberattacks.

Cyber Criminals as State Proxies

Geopolitics is playing a significant and growing role in the evolving pattern of cybercrime. For example, Microsoft estimates that the war in Ukraine has directly impacted 43 other countries in the form of cyberattacks. Robert Hannigan noted that governments are witnessing an increased volume of attacks against critical infrastructure, with criminal groups being sponsored by nation states to act against their geopolitical rivals.

> **"The gloves have come off, if you will."**
>
> - Robert Hannigan

Today's cyber threat actors – whether state-sponsored or 'privateers' – are organized and professional, many deploying specialised negotiators to obtain the best monetary settlement from their victims. Some even possess the criminal equivalent of a 'customer services' team, underlining the quasi-corporate footing many groups operate on.

New Threats, New Targets:

How Secure is Your Supply Chain?

Targeting an organization's supply chain is not a new strategy in cybercrime. The much-publicised 2016 ransomware attack on the Maersk shipping line originated through the company's supply chain, for example.

The key difference today is measured in volume. The supply chain is now far and away the most prominent vector for attack, accounting for some 80% of cybercrime incidents, according to BlueVoyant's Robert Hannigan.

The reason is simple: as corporates improve their own cybersecurity measures, and become more effective in their cyberattack responses, the threat actors have opted to exploit the supply chain as the 'soft underbelly' of the commercial ecosystem.

BlueVoyant's Tom Moore notes:

"There are trusted partners in every organisation's supply chain. They may either have direct, trusted links into your systems or they may simply be critical to your operational continuity. And threat actors don't always operate at one degree removed. It may not necessarily be your supplier, or your supplier's supplier, which is targeted."

With the proliferation of managed service providers, especially relating to outsourced IT services, the contagion from an exploited vulnerability in a single provider has the capacity to spread globally before any client institution is aware of the problem.

Organisations must therefore manage not just their own cyber threat environment, but also ensure visibility, monitoring and protection of all third-party relationships that might offer gateways to cybercriminals. This means incorporating supply chain collaboration into commercial contracts – including retroactively if possible – so that if an incident occurs it will be possible to tunnel through the entire supply chain and stimulate a collaborative response.

The Growing Risk of Regulatory Aftershock

and Why the Financial Sector is in the Spotlight

As some of the most tightly regulated businesses within the global economy, banks and financial services companies are especially vulnerable to regulatory fallout from cybercrime.

At the same time, the investment made in immutable backup and restore systems has created a high level of protection from the twin threats of theft and/or encryption of data which are traditionally associated with ransomware.

These two points are not lost on cybercriminals; in response they are introducing a new and potentially highly damaging third level to many attacks. Tom Moore notes: "Companies can use their backups to resume operations but what they cannot do, once the data is leaked, is put the genie back in the bottle. We're increasingly seeing threat actors contacting customers, investors, and supply chains to notify them of the breach, thus applying additional external pressure to victims."

As a result, in the United States, exposure to litigation is becoming a major loss factor from ransomware attacks. In Europe, meanwhile, regulatory non-compliance – and the penalties incurred – represents a growing burden.

The Regulators are Spreading their Net

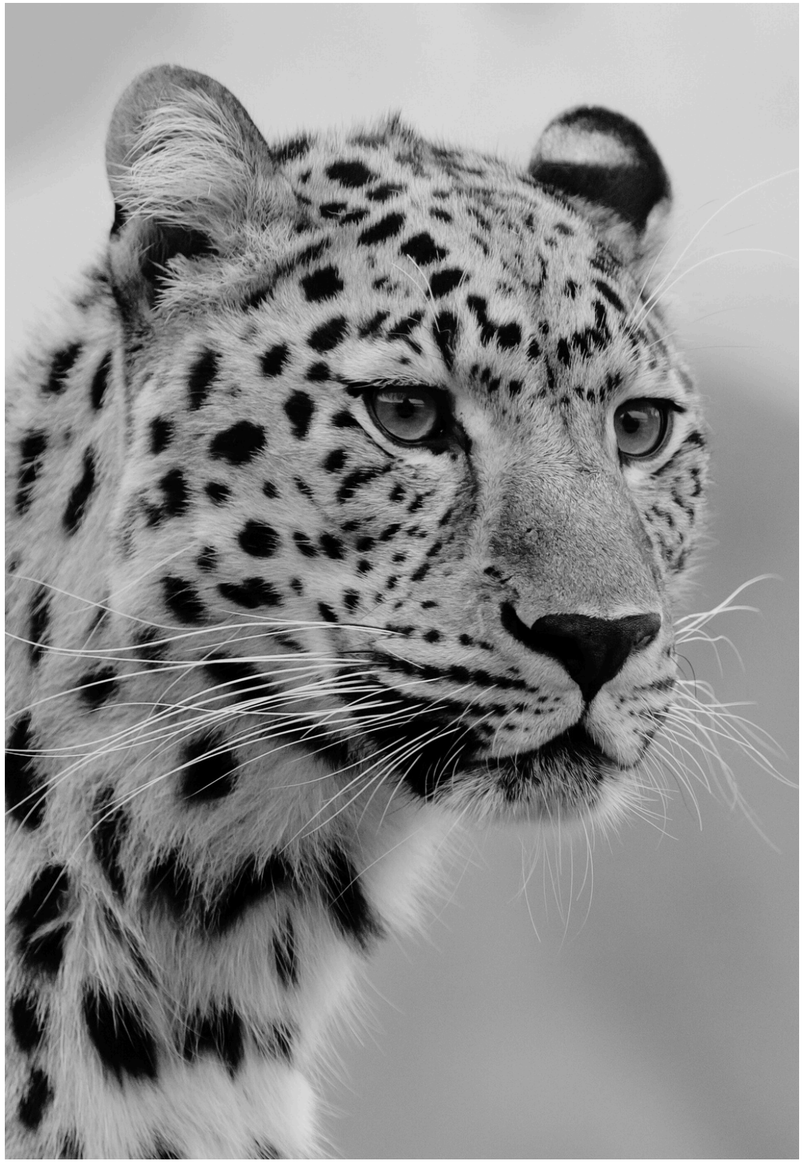
The regulatory environment around cybersecurity is fast evolving and broadening its reach. For example, the European Union has already introduced the NIS2 Directive and Digital Operational Resilience Act (DORA), the latter being directly applicable to financial institutions. Both protocols mandate strict risk management, reporting and management accountability in relation to cybersecurity.

In the UK, legislation mirroring these directives is making its way through Parliament in the form of the Cyber Security and Resilience Bill, with the financial services sector being additionally governed by the FSA/PRA enforced Operational Resilience Framework.

"Whether the threat actor takes your data or not, the moment they have entered your systems it will be perceived as a data breach. And unless you can quantify exactly what the threat actor had access to with some degree of confidence, the regulator will be inclined to assume that the entire system was compromised, and act accordingly."

- Tom Moore

As such, a capacity to deal swiftly, openly and professionally with regulators must form an essential element of an organisation's incident response plan. Using experience gained from his regular liaisons with the UK's Information Commissioner's Office (ICO), Tom Moore recommends providing only verified information on the breach, accompanied by details of the risk mitigation plan emphasising the pre-approved and rehearsed series of actions taking place within the business and/or supply chain.



The Executive Angle:

Cyber-Resilience is a Leadership Function, Not Just a Technology Function

Who owns cybersecurity best practice within a financial services organisation? At Board/leadership level it is essential that clear roles, accountabilities and actions are not just put in place, but also continually rehearsed and refined so that when an issue occurs there is total clarity as to what steps must be taken and by whom.

It is imperative to stakeholder buy-in that incident preparedness exercises are based on realistic scenarios, which reflect the seriousness with which an incident would impact the business. Management time is precious and if the incident being simulated is not deemed mission-critical, minds will wander.

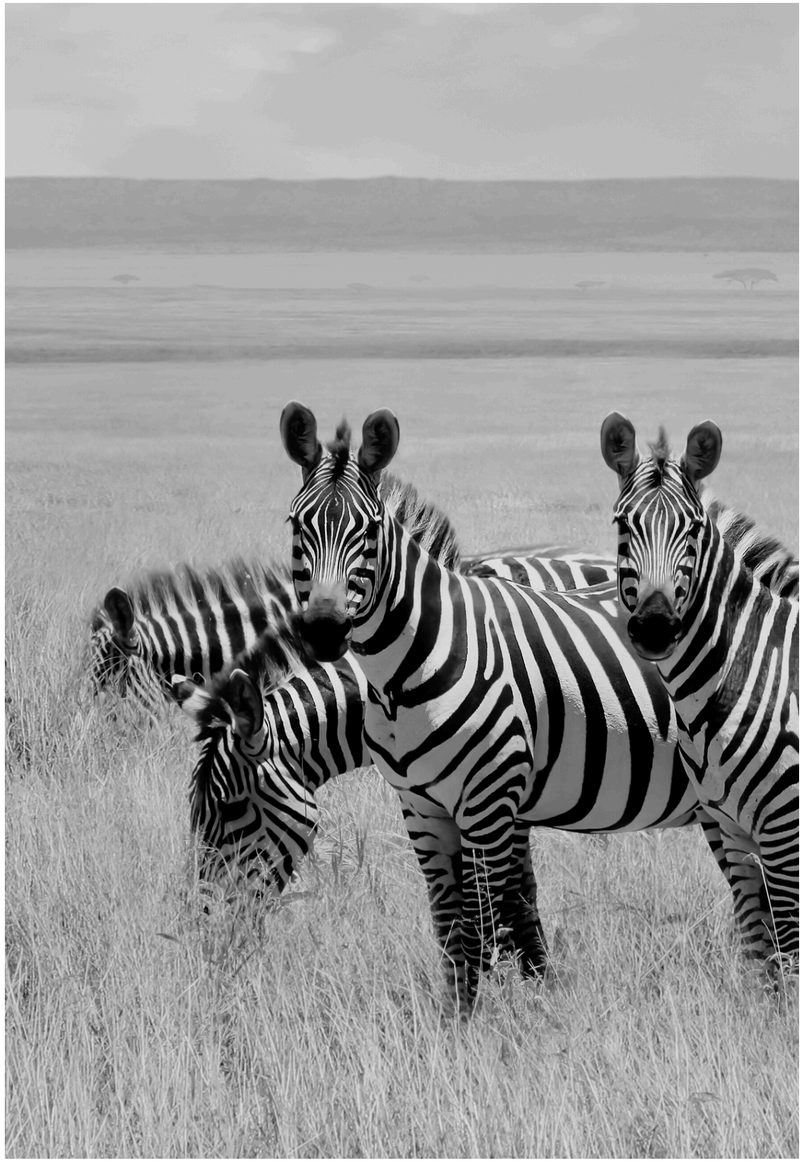
Robert Hannigan notes: "Boards need to see cyber as another key risk factor, alongside financial, operational, health & safety and other risks. When it comes to incident response, there should be somebody at Board or ExCo level who really owns that process and drives it forward. And even if they're not experts in cybersecurity – which they are unlikely to be – this person still needs to know how to challenge their CISO, or the third-party specialists who are managing incident preparedness, including which questions to ask."

Developing organizational 'muscle memory' for incident response can make an important difference to the severity of the eventual outcome.

In the experience of BlueVoyant, an organisation's ability to recover quickly from a ransomware or other cyber attack is around 80% attributable to having a well-rehearsed, usable, practical and fit-for-purpose incident response plan.

That said, attracting cyber-literate talents who can operate at Board-level is not a straightforward task; one which is further complicated in the financial services sector due to the unique regulatory environment in which firms must operate. This is certain to influence the skills and attributes required in the C-suite; something that we at Sayer Haworth are already witnessing in executive search mandates.

> **"Boards need to see cyber as another key risk factor, alongside financial, operational, health & safety and other risks."**
>
> - Robert Hannigan



Friend and Foe:

The Importance of AI to Cybersecurity Attackers and Defenders

Given the all-pervasive impact of artificial intelligence (AI) on global business and commerce, it should be little surprise that the technology is now an important weapon in the arsenals of both cybercriminals and those defending against them.

As with most AI applications, the technology is not being deployed to bring about innovative new threats; instead, it is supercharging existing attack strategies by enabling threat actors to identify and exploit vulnerabilities much more quickly and with greater agility than previously possible.

As an example, by using AI to profile the potential victim in more depth and detail, AI can create much more effective social engineering campaigns. The technology is also being used to automate the conversation between the attacker and their victim, using tailored language that encourages the victim to believe they are dealing with a legitimate counterpart.

“Where an attacker might previously spend three months profiling a company CEO in order to create a social engineering campaign, with the power of AI they can now do this for a million victims almost instantaneously.”

- Tom Moore

At a corporate level, systems and applications powered by AI, notably large language models (LLMs), are vulnerable to data poisoning – a method of cybercrime which is a relatively new phenomenon, but which is growing exponentially. Academic studies have shown that even a small amount of rogue data, if placed within the most vulnerable data sets, can render any information or recommendations drawn from that data as unreliable.

“Finding out when data poisoning has occurred, identifying where it has happened, and then remediating it, is incredibly difficult and something that nobody has quite cracked yet.”

- Robert Hannigan

But while it is undoubtedly strengthening the hand of the cyber attacker, AI also has an important role to play on behalf of the defender.

Firstly, it is improving productivity and driving automation in cyber defence as elsewhere. Indeed, Robert Hannigan sees a time in the future where AI-powered systems could replace the Security Operations Centres (SOCs) operated by larger organisations.

Much more importantly, however, in the same way that AI is supercharging the search for vulnerabilities to be exploited by attackers, so it can be deployed internally to locate and rectify weaknesses in system designs and networks.

Robert Hannigan explains: “What AI can do is refactor code. It can go through and find those vulnerabilities more quickly, thus improving the security of that code before it is rolled out.”

A last word on technology. If AI is today’s cybersecurity focus, then quantum computing may well be tomorrow’s. It remains unclear when the first quantum systems will enter service; but when they do, the consensus is that even the most sophisticated encryption used today will be rendered obsolete. The good news is that quantum-proof mathematical standards are already available, with early adopters including legal and financial services firms. In addition, there’s a growing stable of specialist advisors focused on mitigating the quantum threat.

Conclusion:

Act Now or Suffer Later

Amid today's economic and geopolitical upheaval, anticipating cyber threats is not just prudent, it's a survival imperative.

Increasingly, cybercriminals acting on behalf of nation states are using attacks to undermine public confidence – a version of hybrid warfare that is proving hard to defend against. It means organisations which have hitherto felt themselves safe from cyber attack, due to their relatively small size or through operating in 'everyday' sectors such as leisure or retail, are today being targeted precisely because of the part they play in maintaining public morale. The financial services sector, as the economic cornerstone of any developed country, must acknowledge this enhanced threat level.

The good news is that there is wealth of government support and advice available to financial institutions – much of it free – alongside specialist cybersecurity advisory firms like BlueVoyant and others, who can advise on preventative measures and lend support to incident response.

Business leaders can also play their part by ensuring that cybersecurity is a Board-level priority, deploying best practice based on:

- Clear roles and accountability for dealing with cybersecurity incidents
- Full visibility of supply chain risks and accountabilities
- Developing institutional 'muscle memory' through rigorous and realistic exercises based on severe but plausible scenarios
- Using consolidated threat intelligence to identify and prioritise genuine risks and business outcomes

"There is plenty you can do as a Board. Every day we see companies that are under attack but are resisting those attacks; and even if one gets through, they are isolating the issue and not going out of business, not ceasing to produce."

- Robert Hannigan

About The Contributors

Robert Hannigan
Head of International Business
Europe & Middle East, BlueVoyant

Robert spent most of his career in UK government service, including as Director of GCHQ, where he established the National Cyber Security Centre in 2016. He was also responsible for the UK's offensive cyber programme, with military colleagues. He speaks and writes regularly on cyber and technology issues, including for the BBC and FT. He has been with BlueVoyant since it was founded in 2017.

Tom Moore
Director of Digital Forensics &
Incident Response, BlueVoyant

Tom advises organisations on managing complex cyber incidents, regulatory investigations and corporate security challenges. Since 2001, he has led more than 220 digital forensics investigations across the UK, Europe, the Middle East and South-East Asia, supporting corporate clients, legal advisers, law enforcement agencies and industry regulators.

To discuss any details within this report please contact James Sayer.

SAYER HAWORTH

James Sayer,
Managing Partner

Email: jamessayer@sayerhaworth.com
Tel: +44 (0) 203 751 6260
Mob: +44 (0) 7951 966 077

Sources

CyberSecurityVentures.com