SOPHOS
Cybersecurity evolved.

//eacs

# The Finance Sector and Supply Chain Risk

## Developing a Proactive Cybersecurity Approach

# Contents

# A fragile supply chain

It was the spectacular supply chain attack on one of the world's largest and most trusted technology suppliers that forced its CEO to make an embarrassing admission: the company had suffered an "extremely sophisticated" cyberattack that resulted in it losing data so critical that it had compromised the integrity of a software product upon which thousands of large organisations depended for a fundamental layer of their security.

As a shocked industry took stock, the company told its customers to take urgent action to block attacks exploiting the compromise. Within weeks, reports emerged that several large companies had been targeted using the stolen software, some possibly successfully.

A description of the SolarWinds attack? In fact, the incident described above happened not in 2020 but in 2011 to RSA, then a subsidiary of EMC Corporation. The software in question included the seed values and algorithms used to guarantee the company's SecurID platform, a hardware token considered at the time to be the gold standard for two-factor authentication.

In the end RSA had to replace almost every token in use, around 40 million of them. At a time when SolarWinds is considered a cautionary tale, the events of 2011 serve as a reminder that supply chain attacks are not a new phenomenon even if back then the world optimistically assumed the incident was probably a one-off.

What RSA and SolarWinds illustrate is the importance of multiple trusted supply chains on which companies in every sector, including financial services, build their businesses. In those examples, the chain of trust was a technology, but supply chains can also relate to almost any aspect of any third party organisation or partner, including its processes, resilience, overall security, and employees. The nature of supply chains varies by sector and company but it's still a huge subject to contemplate for anyone whose job it is to worry about security threats.

## SWIFT compromise

In the banking end of financial services, the most instructive example of the diversity of supply chain insecurity might be the infamous 2016 attack on the Bangladesh Bank which allowed the North Korean Lazarus hacking group to siphon $101 million from its accounts. Famously, but for a single typo and sheer luck, the sum lost could have resulted in losses of $1 billion. But what grabbed everyone's attention at the time wasn't the money involved but the way the attackers has comprised SWIFT, an inter-banking messaging system used by every bank to confirm cross-border financial transactions. The Bangladesh Bank attack is only the best known of a series of SWIFT compromises which plagued the system around that time. As with SolarWinds, with no simple alternatives, organisations had to continue trusting something that was clearly only as strong as its weakest link, of which there appeared to be plenty.

## The Codecov attack

Less noticed than SolarWinds, what happened to Codecov in 2021 is an instructive example of how software is turning into the biggest example of a supply chain whose risks are difficult to see. The company, a maker of developer auditing tools, suffered a compromise of its Bash uploader script, potentially allowing attackers to "export information stored in our users' continuous integration (CI) environments," the company announced. "This information was then sent to a third-party server outside of Codecov's infrastructure." Codecov is not a household name but its software is used by 29,000 enterprises around the world, including many banks.

What all these incidents underline is that supply chains and chains of trust are not only inherently risky but difficult to integrate into a risk mitigation strategy. If you can't trust your partners then who can you trust? And even if you don't trust them, how do you interact with them and assess their security?

# Sizing the attack surface

Financial services institutions have become used to the idea that it is menaced by every type of cyberattack going. If cybercriminals come up with an innovation, it is a certainty that the first organisations to experience it will be in this sector. These include not only ones targeting supply chain weaknesses, but traditional threats such as DDoS, business email compromise (BEC), nation state espionage, data breaches, and the inescapable menace of ransomware.

But for the financial sector the real exposure is far greater than a simple list of threats and involves understanding their attack surface. What this means in practical terms is that while the range of threats have grown, the exposure to any one of them is an order of magnitude larger than it was even five years ago. In the past, security at partners and in supply chains was seen as someone else's problem, presumably theirs. Today, nobody is under any illusions that these entities are a part of the attack surface of large entities doing business with them, even if the exact size of this can't always be estimated. The different elements that make up this expanded attacks surface include:

## The tech and dev supply chain

As discussed above, financial organisations have become dependent on a range of technology suppliers at different levels of the software stack. This offers many advantages over legacy platforms but at the cost of a universality that makes it easier for attackers to target a smaller number of applications used across many institutions. There is a growing awareness that some of these layers – hardware firmware, microprocessors used in datacentre and cloud server farms, and proprietary tools used by third-party developers – expose institutions to invisible risks.

## The vulnerability (and patching) boom

According to figures from NIST, in 2020 the number of CVE-level software vulnerabilities added into the National Vulnerability Database (NVD) reached a record high of 18,103, of which 57% could be classified as 'critical'. A growing number were 'no click' and could be exploited without user intervention. Many industries including finance are now shifting from worrying about zero day attacks to focusing on emergency patching (i.e., patching severe public flaws before they are reverse engineered).

## Open Banking APIs and fintech

Open banking and the Revised Payment Service Directive (PSD2) have been promoted as a way of raising the level of innovation in a banking sector not always receptive to new ideas. But as institutions give third party providers (TPPs) access to their data, its security still depends on issues of consumer consent and compliance with regulations. Gartner has predicted that by 2022, abuse of APIs by cybercriminals will become a common type of attack and there is no reason to doubt this.

## Mobile banking apps

The arrival of mobile banking has turned the apps that make it possible into a new category of risk. These can contain vulnerabilities of their own beyond which lies the growing problem of fake banking apps appearing in app stores. More generally, mobile banking depends on third parties, including app developers, mobile networks, device makers and the security of mobile operating systems.

## Nation state attacks

It's easy to discount the fact that as a fundamental layer of the economy, banks are now part of a country's critical infrastructure. This was brought home to the US government in 2015 when Iran allegedly launched a series of DDoS attacks designed to disrupt its banking sector for geo-political reasons. Meanwhile, countries such as North Korea have turned attacking banks into a business model, reportedly training thousands of hackers to target the sector on an ongoing basis.

## Pandemic working from home

The pandemic not only forced millions of people to work from home but prompted cybercriminals to re-double attacks that try to exploit the security weaknesses this created. It looks as if some of this hybrid and home working will persist, which raises the question of how employees will be protected in home environments that are not always conducive to good security. Right now, there is a lack of security tools to monitor user data access let alone protect the numerous devices that use home networks. This probably predicts an era of much greater control over how employees interact with data and devices.

## Exposure to breaches at partners

Loss of data via a third party is a constant worry. In 2017, brokerage Scottrade Bank admitted it had suffered a data breach after a partner uploaded a file in an unprotected state. The same year, 400,000 customers of Italian bank UniCredit had their accounts targeted after a recruiting platform managed by a third party was successfully breached. How much due diligence is done on the data security of third parties deeper in the chain of trust? Currently, nobody knows.

## The customer

It has taken years for banks to come to the realisation that some of their security perimeter exists on the devices and in the minds of their customers. In the case of retail banks, this comprises millions of people whose security state they know nothing about but must assume is poor. This problem is as old as the hills and yet it has not been solved. One way of conceptualising this risk is to say that to protect themselves from customers, banks must somehow develop systems that protect customers from themselves.

## Legacy patching

It's been understood or years that legacy infrastructure is a drag on innovation in financial services, as well as exposing organisations to known and unknown security risks. The problem divides into two areas of concern: the legacy infrastructure specific to banking and financial services, and legacy equipment that might create vulnerabilities among privileged partners. For banks in particular the attack surface offered by legacy systems is potentially huge, taking in networks of ATM machines (many of which run old versions of Windows), databases, and applications used to support tools that can't easily be replaced.  The conventional response to this is a regime of continuous patching and oversight which weighs down organisations with added IT costs. But even when contained, the implications of invisible legacy vulnerabilities in supply chain partners creates an entirely new level of uncertainty.

## Ransomware: less of it but more spectacular

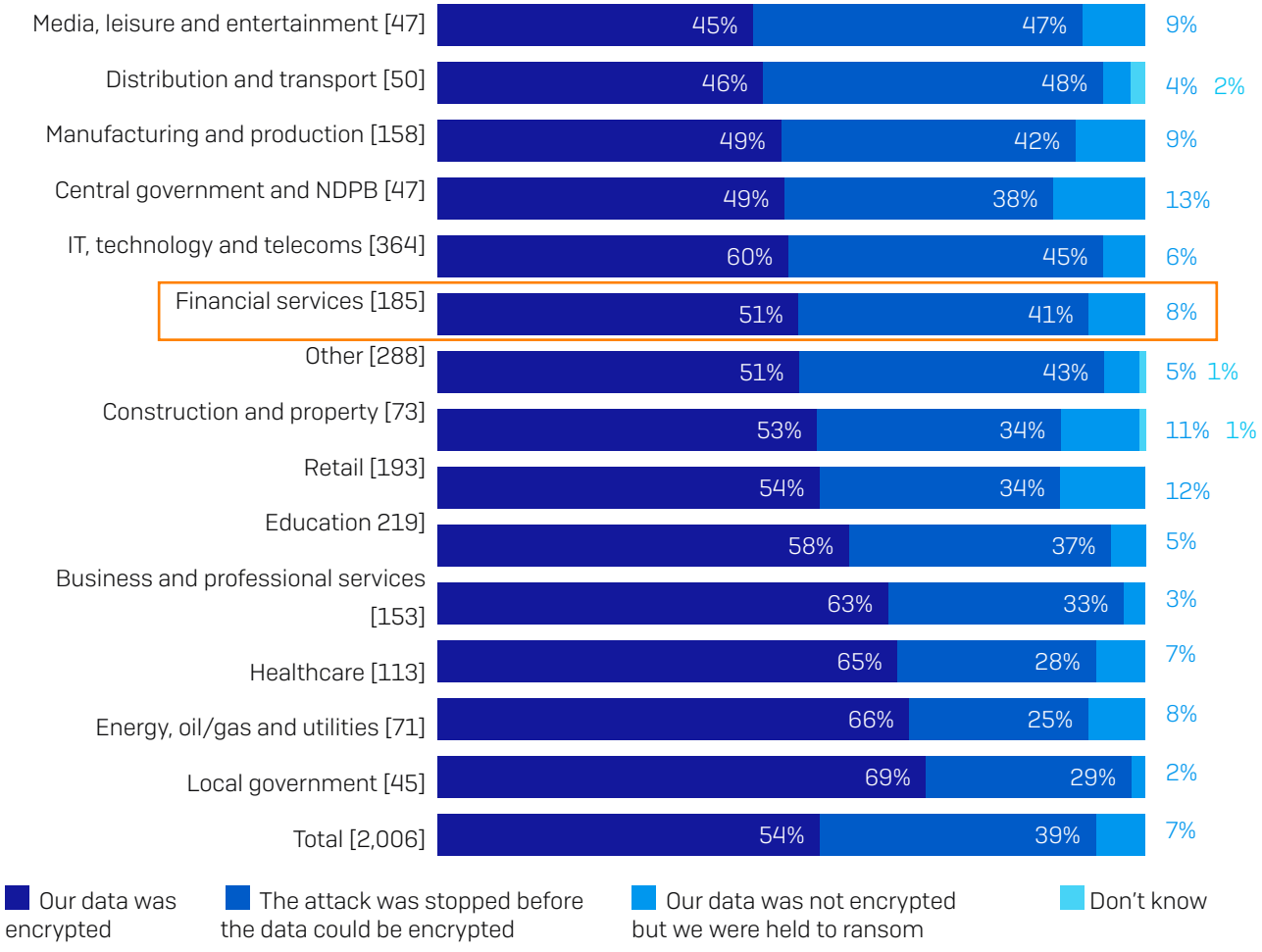
Ransomware is all over today's enterprises like a rash and the victims get bigger with every passing month. But does that mean that it's out of control? Surprisingly, the findings of the Sophos global State of Ransomware Report 2021, which questioned 5,400 IT managers from 30 countries (including 550 in financial services), suggests that organisations have significantly reduced the number of successful attacks. It's just that when things do go wrong, ransom inflation is driving up the financial pain.

In 2017, 54% of respondents said they'd been affected by ransomware in the previous year, which dropped to 51% in 2020 and to 37% in 2021. This partly reflects better defence and mitigation but also, ominously, an important change from generic mass attacks to far more targeted, 'hands-on' keyboard intrusion. If that holds true, this predicts a further drop in compromise volumes next year but at the cost of fewer, more serious breaches. Consistent with this is that 42% of successful ransomware attacks now affect organisations over 1,000 employees compared with only 33% for those of between 100 and 1,000.

Some sectors recorded higher levels of successful encryption than others, ranging from media at one end with 45% to local government at the other which reported that this happened in 69% of cases. For financial services, the figure was in the middle of the pack at 51%, with 41% saying they had been able to stop the attack before this happened. Perhaps significantly, 8% of financial services organisations said data was not encrypted but they'd still been held to ransom. This frequency of this type of scenario is now rising, a sign that attackers are shifting tactics from encryption to threatened data release as their primary extortion tactic.

## Ability to stop encryption varies greatly by sector

When it comes to stopping the encryption of files, some sectors are far more successful than others.



# A view from Morgan Stanley

In May 2021, Sophos invited Rachel Wilson, Head of Cybersecurity for Wealth Management at Morgan Stanley, to chair a webinar discussing the sector's top concerns. Rachel is hugely experienced, her career shaped by 15 years working for the National Security Agency (NSA), during which she was a key advisor in securing the 2012 Olympic Games in London and, more recently, running cyber-exploitation missions against US adversaries.

Now working in the finance industry, the key issues she identified during this session included not only the supply chain but the constant threat from credential theft and exploitation, the impact of pandemic working on security, and the rising threat of nation state attacks against banks.

During the session, 50 financial sector participants were polled on their biggest worries, starting with the issue of remote working patterns and their impact on cybersecurity risk. On that topic, 87% agreed or strongly agreed that remote working increased their cybersecurity risk, with only 13 disagreeing. It sounds like an emphatic result, but Wilson's interpretation was more nuanced.

"I could go any of these directions depending on how well organisations have implemented their remote work setup," she said. "All of these things could be true."

On whether organisations saw developing a supply chain risk strategy as a top priority, 83% agreed or strongly agreed and only 6% flatly disagreed.

As to the threat to these supply chains, Wilson not surprisingly given her background, drew everyone's attention to nation state actors. In the past, these would have been viewed as a threat limited to only certain organisations and sectors, but this was no longer true, she said. What has moved the dial on this are important business changes in the cybercriminal organisations conducting these attacks.

"They work for their government by day and then work as hackers-for-hire in a criminal capacity. It can be difficult to differentiate between what are tools, tactics and techniques associated with a nation state compared with a cybercriminal."

Long predicted, the tools, tactics and techniques of nation state cyberattacks have filtered into the criminal domain, spurring further growth and sophistication. But the influence of this cross-fertilisation in both directions is now apparent.

A curious theme is the return of older threats, Wilson said, with a notable example for banks being the unexpected rise of old-style cheque fraud in the US as a response to Coronavirus restrictions.

"In 20 years in cybercrime, I've never seen anything like what we've seen recently, with a 40% increase in attempted cybercrime globally and in financial services a 240% increase in attacks. Why? Because attackers looking to take advantage of our anxiety and desire for quick solutions."

When asked to rank their biggest workforce concerns during a time of remote working, vulnerabilities in personal devices were a concern for 49% of respondents, followed by the security of home Wi-Fi connectivity on 26%, email misdirection on 18%, and the risk of virtual meetings on 8%.

"I told my board of directors that when we sent everyone home [during the pandemic] I wasn't any more or less worried about cyber and data security than I have been over the last four years. That's because we've adopted a zero trust model where I assume I have no confidence in the security of my employees' devices. So, if even if my employees are doing all the wrong things… we never have any proprietary of client data stored locally on their phones or laptops." In addition, Morgan Stanley uses VPNs for all connectivity with strong multi-factor authentication for everything and everyone.

But she believes one of the most underestimated and simple data threats for financial services is old-fashioned email misdirection. "This is employees sending emails to the personal email address, sending it to an unintended email address, or it might be forwarding that virtual meeting invitation not realising that it contains not only the invite but attachments containing sensitive data."

As for patching, this has become a perpetual emergency organisations must plan for. Developing a strategy to manage unexpected patches should now be a priority, if necessary requiring organisations to take services offline at short notice while they are applied.

"My workforce has got used to the idea that when that patch is released, even if it comes in the middle of the day, if the vulnerability is critical enough we are going to go ahead and reboot every machine across the firm. We don't want to wait a second for that patch to be implemented," said Wilson.

## "On top of everything else over the last 16 months, we have been living through a cybercrime pandemic"

***Rachel Wilson, Head of Cybersecurity for Wealth Management at Morgan Stanley***

## Case study: taking it to the board

It's the struggle that can exhaust even the most resilient IT manager getting boards to invest in security. The return on investment is difficult to quantify, the need sometimes as obscure and hard to explain as the threats themselves.  Security spending ends up as an Oliver Twist, perpetually coming back for another helping.

In the case of a large, anonymous Sophos customer in financial services, the answer was to get someone else to explain the problems for them. The opportunity arrived two years ago after a high-profile red team wargaming exercise which uncovered weaknesses best presented by the people who'd found them.

"We got penetration testers to present to present to the board," says a senior member of the company's inhouse SoC team, admitting they had "chanced their arm." But it got results. "They explained in graphic detail the implications of different things being compromised. Previously, there was always a concern that telling the story that there was a gap or vulnerability here or there could get diluted." In a theatrical finale, the pen testers were even able to show the chief executive a photograph of one of their staff sitting in his office. The chief executive's reaction? Suitably livid.

"Historically, we'd send them a board pack detailing pen test attacks, but we were often concerned that either they didn't have time or didn't digest it fully. We thought if we can get the pen testers to tell the story if might do the trick. It was received very well and has become an annual event the executives look forward to."

But occasionally pen testing can reveal things about partners that are trickier to process such as the time a vulnerability unexpectedly gave testers access to a service provider's network. "It was the fact we could get there. That caused some friction and we had people throwing the Computer Misuse Act at us."

By contrast, third parties with access to the institution's network must as a basic minimum provide assurance in the form of pen testing reports. Nevertheless, extreme steps are sometimes necessary such as the case of a breached partner company that caused enough worry that the institution's CISO agreed to rapidly shut down of all connectivity as a precaution. "We put all their emails in a quarantine until we got reliable information. We basically don't trust anyone. It's sheer paranoia."

The growing risk from partners is a new layer of worry on top of all the other threats that a large financial organisation must contend with. Often the line between maintaining stability and a critical failure is a fine one, with ransomware attacks offering a good example. "We had a very narrow miss where someone had received and opened the document. The only reasons we got away with it was because the software required for it to run didn't exist on that machine and so it didn't execute."

Targeted attacks are another pest. "We had one torrid summer when we were getting a lot of whaling attacks. Our assumption is that the higher up the organisation a target is, the less likely these individuals would think things through. For example, our contact centre staff are very savvy as far as phishing attacks go, whereas further up, they're slightly less so."

"There are only five people in the organisation who have access to USB." Meanwhile, only named people can access media such as CD drives, which is legally required for things like police access to data.

"We don't allow emails with executables and we don't allow things like old Excel formats. With the exception of a tiny number of people who needed access to archives, there is no requirement in the organisation for Java."

> "In an institution where data security is the crown jewels, it becomes necessary to lock down everything, starting with simple things like USB."
>
> ***Sophos Financial Services Customer***

# Supply chain recommendations

Supply chain risks manifest across a range of third parties, including outsourced and professional services, Managed Service Providers (MSPs), and project developers, all of which are vulnerable to phishing attacks, malicious insiders, compromised software, and careless data misconfiguration. But how can financial services organisations protect themselves from risks they can't see?

1. **Plan for disaster** proactively by assuming the compromise has already happened. This requires the support of security partners and technologies.
2. **Monitor** legitimate identities and accounts for compromise. The principles of zero trust must extend to everyone and everything, including internal users as well as external ones.
3. **Audit** your entire supply chain, including information on their supply chains in this process. Treat any access these provides have to your systems to be subject to the same limitations that apply to individuals by imposing access restrictions.
4. **Assess** which certifications and compliance requirements each supplier must confirm to, including SOC 2/2+/3 for cloud providers. Audits alone don't guarantee anything which is why asking for penetration and red team test results can be necessary to do business with a partner. They should be expecting this sort of request from a bank.
5. What is the bare minimum for supplier connections? Because the abuse of privileged credentials is rampant, multi-factor authentication (MFA) is an absolute must. Similarly, access via RDP and VPNs should be **treated as luxuries** given out sparingly. Again, MFA is essential combined with careful monitoring of these entry points.
6. What sort of patching, remediation and reporting policies does a third-party have? In case the supplier suffers an issue, making sure your company is prioritised on the **'need to know' list** and being informed is part of the contract. Make sure the people who negotiate these relationships at that level understand the importance of this issue.
7. Most important of all, **treat the supply chain as a high-risk user** rather than a hypothetical risk. Failing to do so risks putting your organisation on the receiving end of someone else's security failures.

## Further reading and resources

A good starting place for organisations trying to get on top of supply chain and risks is NIST's SP 800-207, Zero Trust Architecture.

**Sophos Whitepapers:**

Minimizing the risk of supply chain attacks – best practice guidelines

Securing your supply chain from third party risk

Demystifying Zero Trust

**Sophos Products:**

Sophos Managed Threat Response

Sophos Rapid Response

Sophos XG Firewall

Sophos Phish Threat

Sophos Endpoint Detection and Response (EDR)



2021-06-08 (WP-EN-PS)

//eacs

SOPHOS