CISO EXPERT PERSPECTIVES REPORT

CROSSWORD
CYBERSECURITY

CISO EXPERT PERSPECTIVES REPORT

EXECUTIVE SUMMARY

Stuart Jubb, Group Managing Director, Crossword Cybersecurity

Scarcely a day goes by without more headlines about cyber-attacks. And as businesses become better defended, attackers are turning their attention to weaknesses in the wider supply chain. An attack on Zellis, a payroll services provider, for example, led to security breaches at firms including British Airways and Boots[1]. The critical vulnerability affecting the MOVEit Transfer file-transfer application[2], exposed at the beginning of June 2023, poses a risk to thousands of companies and millions of developers, according to analysts.

Advances in artificial intelligence (AI) tools will help improve cybersecurity by automating tasks such as filtering alerts to find the ones that need immediate action and monitoring behaviour on networks to identify anything out of the ordinary. However, these tools are available to attackers as well – and evidence shows they are already incorporating them. Hackers are using AI to write more effective phishing emails[3], for example, and much like legitimate businesses, they are exploring ways that AI can automate entire parts of their operations. As always, cybersecurity is an ongoing arms race.

Because how we secure the supply chain is a topic of vital, unwavering importance, we interviewed several senior cybersecurity professionals from various sectors to assess the current state of play. We asked about the challenges to improving supply-chain cybersecurity in their sector and the implications of growing regulation, as well as the processes they recommend for third-party assurance. We also asked them what they believe different sectors can learn from each other, and to what extent organisations should and do collaborate against cyber-attacks.

ESTABLISHING A PROCESS

Their answers, set out in this report, make for fascinating reading. One significant finding was that several things that should be happening are not – or at least not enough. For example, we heard that the cybersecurity team should be included in the assurance process from the outset. Too often, that does not happen. Similarly, some respondents said they were aware of many businesses that didn't have a clear view of their supply chain at all.

The need for a strong and consistent cybersecurity process was a recurring theme. This usually entails a ranking system of some kind to ensure critical suppliers are thoroughly evaluated for security risk, while the lowest-risk suppliers receive more basic checks. Another recurring theme was the need for a positive attitude towards regulation. Most of those we spoke to felt that regulators help companies by establishing an obligatory base level of security and that standards established in regulated sectors sometimes filter through into others, lifting them, too.

TIME IS OF THE **ESSENCE**

A couple of other elements stood out to me. First, companies that are also suppliers have a mixed view of security practice. On the one hand, they need to secure their own supply chain, so they understand the need for assurance processes. But on the other, as suppliers themselves, they are obliged to undertake an assurance process that too often is onerous and poorly thought out. One respondent told us that customers frequently send out long questionnaires, with lots of questions that require research yet prove irrelevant. A lot of time can be wasted that way and businesses might need to consider whether the burden they place on suppliers is reasonable.

Second, I was struck by the need to pay close attention to the particular challenges that arise in supply-chain cybersecurity, which vary according to the size of organisation. For start-ups and charities, it can be a challenge simply to bring together the resources needed to assess the supply chain. Large companies, on the other hand, have the resources but struggle to cope with its scale. Wherever you sit on the spectrum, supply-chain security simply isn't easy to manage.

When it comes to increasing supply-chain resilience, time is of the essence. For many organisations, the biggest hurdle is knowing where to start, particularly when faced with a complex supply chain involving thousands of vendors. Navigating an expanding range of regulations and dealing with a bewildering array of frameworks and guidance can make the task feel insurmountable.

But there is always a way forward. A willingness to invest in supply-chain cybersecurity is the starting point for a well-defined and effective process, and this report contains suggestions for many other practical steps to take. Like any other cybersecurity challenge, supply-chain security requires constant monitoring and assessment – but it is achievable. We hope this report helps businesses see the wood from the trees and define a way forward.

[1] https://www.ft.com/content/83ae048c-5607-49ae-8786-84f1b8d6cbd8

[2] https://www.scmagazine.com/news/data-security/millions-users-vulnerable-zero-day-moveit-file-transfer-app

[3] https://www.cnbc.com/2023/06/08/ai-is-helping-hackers-make-better-phishing-emails.html

CONTACT CROSSWORD CYBERSECURITY PLC

☎ **+44 20 3953 8460** ✉ **info@crosswordcybersecurity.com**

Capital Tower, 8th Floor, 91 Waterloo Rd, South Bank, London SE1 8RT

1.

RELATIONSHIP BUILDING IS KEY FOR CISOS AT GROWING FIRMS

Cybersecurity due diligence can be onerous for small and growing companies, writes Clair Phelps, CISO at Wagestream. A more standardised approach would help

Start-ups and growing companies face unique challenges when it comes to supply-chain cybersecurity. With limited staff and resources, we simultaneously need to ensure that suppliers meet our security standards, while reassuring customers that we meet their standards, too.

A 'due diligence industry' has evolved around cybersecurity and much of it involves showing the regulator that a company has acted responsibly should a security incident and/or data breach occur. As a supplier ourselves, we must fill out numerous due diligence questionnaires that can contain hundreds of questions – some of which are not even relevant to us as a cloud-hosted SaaS company – and each is slightly different, so we can't simply copy answers from previous ones.

Many companies have independent ISO 27001 and SOC 2 certifications that demonstrate their attention to cybersecurity, but they worry that these alone will not be sufficient proof that appropriate due diligence has been conducted should there be a regulator investigation. Ideally, regulators should give clear guidance to say that ISO 27001 and SOC 2 are sufficient to indicate that cybersecurity standards have been achieved. Instead, as a supplier, we spend valuable time on questionnaires that cover the same ground as the certification we have already.

Cybersecurity assessments could certainly benefit from a more streamlined approach.

BUILDING STRONG RELATIONSHIPS

Another issue is the presence of legacy systems in our supply chain. While people typically associate legacy with systems that are decades old, even relatively recent tools can become legacy if they don't support modern security features. These outdated tools may harbour vulnerabilities from the time when they were created, potentially due to a lapse in controls relating to software development, and could pose a significant risk to our data security.

Building a strong relationship with suppliers and engaging in regular dialogue is essential in tackling supplier risks – far more so than simply relying on a point-in-time security questionnaire. Plus you already have a relationship established if something goes wrong. To facilitate this, a relationship manager in our team regularly discusses cybersecurity concerns with key smaller suppliers, enquiring about vulnerabilities and controls in the face of emerging threats.

However, this approach can be challenging with larger companies, particularly industry leaders, where establishing a personal relationship may not be possible. Indeed, some don't allow auditing and won't answer individual queries about security. The onus is on you to check their security centre for their external auditing and certification results.

FINDING RELEVANT INFORMATION

Information sharing in the cybersecurity landscape is another area that could be improved. While there are paid services available, these can be expensive. In many cases, free alternatives such as Google News alerts can be just as effective for flagging new threats or an emerging vulnerability or even to discover that a supplier has suffered a data incident.

Peer networks offer another valuable resource, but they must be sought out independently. Start-up CEOs often benefit from connections provided by their investors, who link them to other companies in their portfolio. It would be beneficial to have similar support for cybersecurity, as it presents a distinct challenge for start-ups.

Cybersecurity is not always easy to navigate as a small firm. A more relationship-driven approach can help smooth the way when problems arise, but we would welcome more standardised cybersecurity assurance processes as a baseline.

2.

FROM NEGLECT TO NECESSITY:
PRIORITISING SUPPLY-CHAIN SECURITY

Careful supplier evaluation and a willingness to invest are critical to making your supply chain secure against cyberattacks, argues Peter Cooper, CISO at 10x Banking

Supply-chain cybersecurity was once a glaring weakness in the business world. Until about five years ago, it didn't receive the attention it deserved. Many software supply chains lacked built-in security measures and visibility into the intricacies of these chains was hard to come by. While contracts often included some level of due diligence, it was typically focused more on financial aspects than security concerns.

Fortunately, the situation is beginning to change, though the work is far from over. Many of today's business ecosystems still lack security at their core. A single project might have as many as 60,000 separate inputs, very few of which undergo any form of security assessment. No one truly works in a silo anymore. The sheer scale of these supply chains presents a daunting challenge for businesses and for regulators.

EVALUATING SUPPLIERS

The growth of regulation has had a positive effect on supply-chain cybersecurity, though the most prescriptive regulation applies only to sectors such as finance. Many suppliers in these industries inherit the regulatory responsibilities of their clients. However, it is nearly impossible for a single regulator to cover every supplier involved in a particular sector, so they naturally focus on larger suppliers and give less attention to smaller ones.

An effective cybersecurity strategy depends on both financial resources and the will to invest. Technical assurance activities, such as validating a supplier's inbuilt security, can be costly and difficult to implement. Consequently, we tend to reserve these measures for the most vital components. For instance, while we wouldn't spend money on penetration testing for our printers, securing sensitive client transaction data is essential, so we must budget for that.

When it comes to promises about security, don't expect vendors to highlight or address all the risks. For example, many vendors claim their solutions can decrease the risk of security compromise, but many risks stem from mistakes rather than targeted attacks, so the solution will have its limits. Vendors are therefore naturally hesitant to provide a confidence level in their security measures, so it's important to assess them before you buy and be sure they meet your needs.

COST IS CRITICAL

To address these challenges, businesses must establish a clear process for evaluating suppliers and ensuring that their services align with the company's risk appetite. While assurance can never be perfect, a well-defined process goes a long way in mitigating risk.

Having proper security measures in place is the right thing for the business and its customers. However, it is more feasible in sectors with larger budgets. Cost remains a concern. Low-margin and under-resourced sectors like healthcare struggle to afford the tools and techniques that could improve their cybersecurity.

We live in a deeply interconnected world. As cyber risks evolve, it will be ever more important to prioritise supply-chain cybersecurity across all sectors. As the saying goes, a chain is only as strong as its weakest link.

As cyber risks evolve, it will be ever more important to prioritise supply-chain cybersecurity across all sectors.

3.

FRONTLINE RESPONSE:
PROTECTING HUMANITARIAN ORGANISATIONS IN A DIGITAL AGE

Resource constraints and human rights checks add extra layers of complexity to the cybersecurity landscape for charities, says Alex Godoi, Information Security GRC Lead at Oxfam GB

The humanitarian sector faces unique cybersecurity challenges. We are often targets for ransomware attacks from cybercriminals seeking to steal or extort money. At other times, we must defend against rogue states attempting to undermine our work.

That work often takes place in the aftermath of natural disasters or in areas of unrest, which makes cybersecurity even more challenging. Throughout, we must keep our workers safe in high-risk areas, as well as protect the privacy of our project participants.

TRANSPARENCY MATTERS

Getting the right defences in place is not easy because resources are always constrained in the humanitarian sector. As a charity, we may lack the resources to buy every security tool we might need or to attract top talent, who can command high salaries in the private sector.

When partnering with vendors, we must consider not only their technological capabilities but also their human rights record. That can be challenging if they are not transparent about their activities. For example, if we partnered with a cloud storage provider that turned out to be providing surveillance technology to repressive regimes, that would harm our reputation and potentially put staff and project participants at risk if there was a data leak.

Regulations and standards provide a vital baseline for cybersecurity and help build trust between organisations and suppliers. For example, Cyber Essentials Plus is a positive step, but it only really covers the basics. It doesn't require companies to put in place any controls for protecting personal data, such as encryption, nor does it ensure that suppliers audit their own supply chains for cybersecurity gaps. The Centre for Internet Security Critical Security Controls list is a notable exception, as it requires companies to evaluate service providers who hold sensitive data to ensure they have appropriate protections in place.

THE NEED FOR QUESTIONNAIRES

To tackle these challenges, we have developed an internal assurance process. First, we evaluate project requirements and perform a risk assessment to determine where security risks might occur if, for example, we will be transferring sensitive data. During the tendering stage, we send out a questionnaire developed by us to help gauge a vendor's cybersecurity maturity. It covers topics such as their information security policy, certifications, patching frequency, vulnerability testing and assessment methods, and asks about their own suppliers. We want to understand the potential reach of our data within their supply chain.

Based on their responses, we assign each vendor a score. While having a high score carries significant weight in the selection process, it is not the only factor we consider when choosing a vendor for a project. For example, we might also consider a vendor's experience working in conflict zones or their ability to provide on-the-ground support in remote locations. We re-evaluate our vendors annually to ensure they maintain their certifications and address any new vulnerabilities.

Navigating the complexities of cybersecurity requires a comprehensive and balanced approach. Our internal assurance process, which emphasises both cybersecurity maturity and human rights records, allows us to build trust with suppliers while protecting our organisation and its stakeholders as we deliver the crucial humanitarian services that define our mission.

When partnering with vendors, we must consider not only their technological capabilities but also their human rights record.

4.

FROM PROCUREMENT TO PARTNERSHIP: INVOLVE CYBERSECURITY THROUGHOUT

Helen Rabe, CISO at the BBC, on the importance of collaboration through the supplier procurement process and beyond

The cybersecurity team's involvement in supplier assurance should begin in the procurement phase, but all too often we aren't included in initial discussions. That's a problem because the procurement team often don't have the necessary cybersecurity expertise. They might do some cursory checks, but sometimes they don't consider security at all, leaving organisations vulnerable.

The result is that potential risks, such as data sharing with third parties, might not be factored in. To take an example from another sector, a life-sciences company might replace its microscopes with ones that have built-in internet connectivity. The cybersecurity team would immediately ask whether data is shared with the supplier and, if so, what the implications are for security and intellectual property. The procurement team might not consider those risks.

BEFORE THE CONTRACT IS SIGNED

All sectors have instances like that, which leave cybersecurity teams trying to retrofit security measures after the deal has been signed. This could be avoided if, at a minimum, service delivery managers and systems architects were involved during the procurement stage to highlight potential risks and review contracts.

Once the contract is signed, the experience varies depending on the supplier. With large suppliers, it's easy for our concerns to get lost in the noise. We can be treated as a number. That's understandable to an extent, because these firms have countless customers, but it can be frustrating if you are trying to get help configuring a service to the specific needs of your business or trying to manage the risk exposure of critical data.

Again, if cybersecurity wasn't involved in the contract phase, then we might find ourselves with a disconnect on accountability. For example, one supplier might expect you to secure the application layer in a cloud service yourself, while the business teams assume it to be the supplier's responsibility. The shared-responsibility model for cloud services often causes challenges post contract approval.

MANAGING THE RELATIONSHIP

Of course, there are two sides to a contract and we have our role to play, too. Cybersecurity teams can falter in their assurance controls after the contract is signed if we don't do our part to maintain the relationship. That's a matter of resources; it's easy to get caught up in firefighting in cybersecurity. But even if we can't evaluate hundreds of third parties every year, we can prioritise them and focus our attention on the most business-critical items, such as sensitive data sharing with third-party suppliers or identity and access management services.

Coping with many suppliers requires a security service management team who can be much more proactive about managing relationships and contracted assurance controls, for example by making sure service levels are maintained and that annual attestation is reviewed as contracted. Not every organisation is large enough to have specialists for that role, but it's essential when you deal with many suppliers.

By involving cybersecurity teams from the outset, organisations can avoid costly retrofitting measures and foster stronger, more informed relationships with suppliers. Ultimately, a proactive, collaborative approach between procurement and cybersecurity teams is essential for navigating the complexities of supplier assurance and safeguarding assets, providing a more secure foundation for long-term success.

Coping with many suppliers requires a security service management team who can be much more proactive about managing relationships...

5.

‘SECURITY IS A QUESTION OF BALANCE’

Stuart Frost, Head of Enterprise Security and Risk Management within the UK’s Civil Service, explains how he ranks suppliers in order to manage security risks

Supply-chain security is critical in business today. We live in a converged world that is connecting all organisations and significantly increasing the attack surface. An attack on our third parties can be an attack on us, so we need effective management of this increased risk and complexity.

This is a challenge I face daily and one that extends well beyond cybersecurity to include other types of security including information, IT, personnel and physical. Our burgeoning use of third parties also increases the possibility of control gaps, providing many more opportunities for threat actors. However, there are ways to mitigate that risk.

GOVERNANCE IS KEY

A good starting point is to separate suppliers into tiers, such as gold, silver and bronze. Gold-tier suppliers are pivotal to the delivery of business-critical processes. If one of these is breached, then an organisation may not be able to deliver its core objectives. A breached silver supplier would be a problem, but would not necessarily stop us doing business. Finally, a bronze supplier, such as a company providing stationery supplies, would cause inconvenience if it were breached, but would not necessarily jump to the top of our priorities. Obviously, every organisation will prioritise slightly differently.

Governance is key, as it is with many things; get that right and everything falls into place. Every supplier may say their controls are sufficient, but we must assure ourselves of that. At the tender stage that means identifying what security standards a supplier should meet based on the service they are bidding for. They must then provide evidence for their claims and identify what controls they deploy. When the service is in place, we should repeat our assessments annually.

MANAGING THE RELATIONSHIP

Independent assurance, such as the ISO certification (International Organisation for Standardisation) or SOC 2 (System and Organization Controls) reports, are ideal. However, many suppliers are small companies that might not be able to invest in reports such as these. Cyber Essentials and Cyber Essentials Plus, UK government-backed cybersecurity assessment programmes, can be good alternatives, but not enough businesses have these certifications. Worryingly, latest figures show that only 13 per cent of suppliers have assessed the risks of their first-tier suppliers.

Ultimately, supply-chain security requires constant attention, with the same focus we give to our own organisation. We can set requirements for suppliers, but we must also think about the layer of suppliers beyond that and so on. First-tier suppliers should be assuring their own suppliers in the same way.

Of course, security is only one element considered when awarding contracts, so it is inevitable that some will be awarded with control gaps. In these cases, it is essential that the risk is fully understood, accepted and effectively managed. Risk is about creating value and supporting safe-enough delivery of business objectives. An effective governance regime is the tool to create that balance.

Our burgeoning use of third parties also increases the possibility of control gaps, providing many more opportunities for threat actors.

6.

COLLABORATION AND COMPLIANCE:
THE CHALLENGE OF SUPPLY-CHAIN RISK ASSURANCE

Laura Greenwood, Associate Director, Third Party Risk at Crossword, explains why supply-chain security is harder for some sectors, and offers a four-step strategy for success

The software supply chain is hugely complex, with companies often dealing with tens of thousands of suppliers. Stolen software certificates, pre-installed malware and malicious code are rife, and too many businesses simply don't have a grip on their supply-chain risk.

We aren't sector-specific at Crossword, so have a clear view of the differences between sectors – for example, those just getting started and others who are adept at digital transformation. However, the pace of technical development remains aggressive, which can lead to unidentified vulnerabilities at all levels of the supply chain.

LEVELS OF MATURITY ACROSS INDUSTRIES

Ransomware is a massive threat in manufacturing. Attacks increased by 50 per cent [KB1] last year, making the sector the biggest target. A particular risk is the gap between information technology (IT), which covers things such as computers and servers, and operational technology (OT), which refers to industrial equipment and its control systems. Machinery has a long lifespan, so it often runs on old, and therefore vulnerable, operating systems. We've seen machines running Windows NT, which hasn't been supported in almost 20 years. An attack on OT can often spread to IT, causing expensive downtime for the business.

In contrast, the financial services sector is a leader in supply-chain risk; most companies are capable and working on increasing their maturity. They are likely to have a good understanding of the businesses in their supply chain and the resulting risk, and they perform regular assessments to make sure those risks haven't changed. Their heightened awareness reflects the fact that this sector tends to be an early adopter of new technology, so companies within it need to be highly alert to emerging risks, especially as they adopt advances such as artificial intelligence.

A key reason for the maturity of financial services is that the sector is heavily regulated. Regulation sets a baseline and often provides some roadmap of the steps towards compliance. That's a positive influence, though it can be challenging for multinationals to manage compliance with multiple different, and complex, regulatory regimes.

GREATER COMMUNICATION

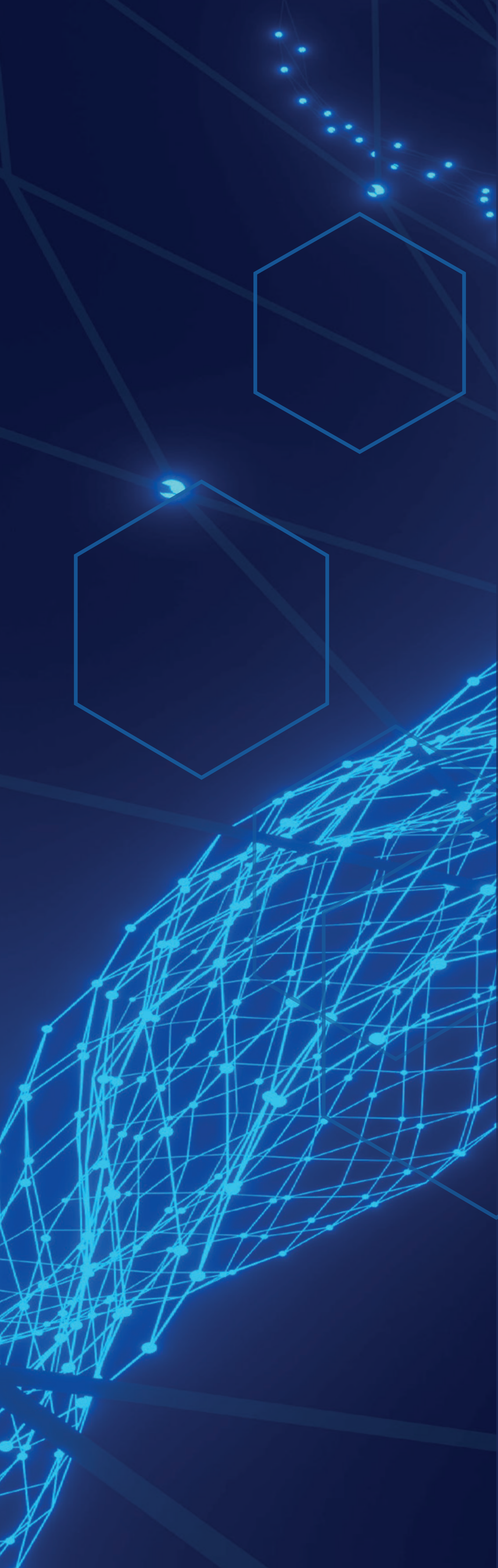
Each organisation approaches compliance individually, which means effort is duplicated. When assessing supply-chain risk, it would be beneficial if there was an independent third party that could evaluate suppliers and give them a risk score. There have been unsuccessful attempts at collaboration between firms in the past. However, the European Union's Digital Operational Resilience Act (DORA), which applies to financial services organisations doing business within the EU and entered a two-year implementation period in January 2023, does contain requirements for sharing information such as indicators of compromise (IoC) or techniques and tactics of cyber attackers with other financial entities. And there is growing consensus that organisations from all sectors can and should work together to tackle cyber threats.

There is always room to improve, even for businesses whose supply-chain security has reached a good level of maturity. But for businesses that are just getting started, I would suggest four broad steps to try to address the problem:

- Figure out what your current situation is and what level of maturity you want to reach. Companies with only basic cyber hygiene might set an immediate goal to additionally cover elements such as real-time monitoring and regular risk assessments. A company which is already doing that might look to commit to more proactive and advanced cybersecurity measures.
- Catalogue your suppliers, with particular focus on those that can access your data or infrastructure. That will help you identify high-risk suppliers.
- Secure management and stakeholder buy-in to your security goals by telling your story and showing how you add value to the business.
- Automate where you can. Supply-chain security is too complex to manage manually, so find tools to simplify the task.

Supply-chain security can feel like an overwhelming challenge, but it is vital that firms address it. The more proactive each company is, the safer the entire supply chain will become.

[KB1](https://www.kroll.com/-/media/kroll-images/pdfs/q4-2022-threat-landscape-report.pdf



Crossword Cybersecurity provides full service expert cybersecurity solutions to proactively reduce risk, without adding any complexity.

One of our core focus areas is within Supply Chain Cyber and we have a dedicated in-house practice which provides a unique solution of services and products, which is designed to make your Third Party Risk Management programme simple, yet effective.

If you would like to know more, get in touch with one of our experts today.

CONTACT CROSSWORD CYBERSECURITY PLC

☎ **+44 20 3953 8460**

✉ **info@crosswordcybersecurity.com**

📍 Capital Tower, 8th Floor,
91 Waterloo Rd,
South Bank,
London
SE1 8RT

CROSSWORD
CYBERSECURITY