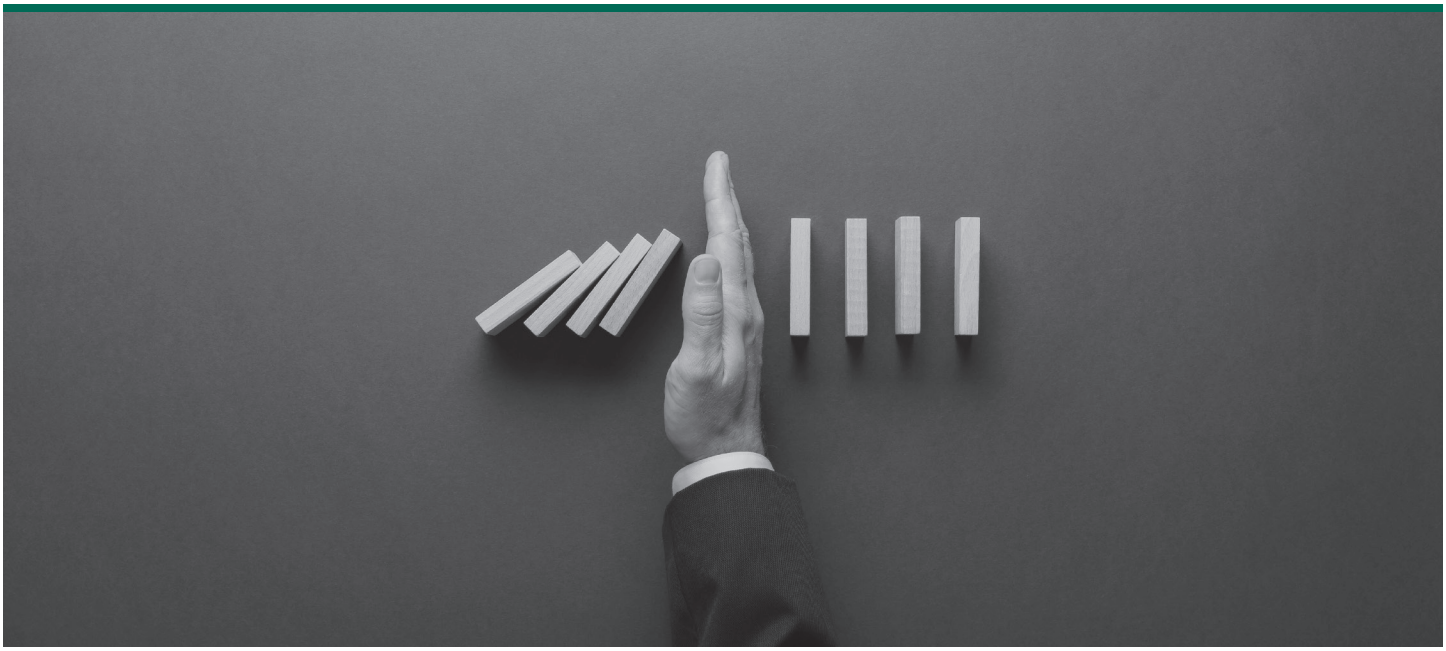
FORTRA

GUIDE *(Clearswift)*

Managing Cybersecurity Risk in the Supply Chain



Supply Chains – Today's Fastest Growing Cybersecurity Threat

Modern business is based on collaboration and partnerships. The global business ecosystem is more interconnected than it has ever been, and supply chains are a vital part of that, enabling organizations to pursue close, collaborative relationships with their suppliers.

However, this has led to increased cyber threats when organizations expose their networks to their supply chain, and it only takes one supplier's cybersecurity vulnerabilities to bring a business to its knees. The old adage of 'you are only as strong as your weakest link' has never been truer. Why would a hacker target 1,000 different organizations individually when it could take them all down with one carefully targeted attack? Governments around the world have highlighted supply chains as an area for urgent attention in tackling cyber risk in 2022 and beyond. But it's a complex challenge that requires collective thought and action from government, business, and cybersecurity providers, to help organizations establish effective control and oversight of their supply chain.

This is because breaches originating in third parties are common and costly. There are many areas of vulnerability in a supply chain, but one of the biggest is via email. Despite the rise in collaborative working tools such as Teams and Zoom, the primary means of communication across a supply chain remains email, and this is often where attackers will target first.

Supply chain cybersecurity threat has grown into perhaps one of the greatest that the world is facing. This guide looks at how the attack surface has changed in the post-COVID world and the impact that the subsequent increase in remote working will have in the longer term. It looks at the verticals that are heavily targeted from a cybersecurity supply chain threat perspective and how organizations can best tackle this challenge by incorporating a comprehensive cyber and email security strategy.

SecureLinkreports that 58% of FS businesses have suffered a breach via a third party, and 55% of healthcare businesses, the two highest sectors

The Current Threat Landscape

Unfortunately, wherever there is disruption, cyber criminals see opportunity. This has never been so clearly illustrated as it was in 2020 and 2021, when the global coronavirus pandemic took hold. Alongside the devasting health and economic impacts, there was also a huge escalation in ransomware, phishing, and island-hopping attacks, as organizations shifted employees to working from home. Stretched security teams were challenged to rapidly deploy robust remote working facilities to maintain productivity which was a huge distraction, one that didn't go unnoticed by cyber criminals.

While coronavirus has thankfully subsided, that doesn't mean that the current threat landscape is much brighter. Most organizations now operate some form of hybrid working policy, while others are fully remote. Either way, the challenges around securing home workers remain. When you also factor in the war in Eastern Europe and the cost-of-living crisis that threatens to overwhelm businesses and consumers all over the world, there is much for cyber criminals to exploit.

These provide ample opportunities for social-engineering attacks. Response-based attacks targeting corporate inboxes are at their highest volume since 2020, according to the latest Quarterly Threat Trends & Intelligence Report from Agari and PhishLabs, part of the Fortra cybersecurity portfolio. Such attacks - that rely on victims responding through a chosen channel of communication and comprise methods such as phishing and advance-fee fraud - represented 41 percent of all email-based scams targeting employees, during Q2 of 2022.

Attacks are becoming not only more frequent, but more sophisticated too. As modular and more extensive malware has become ubiquitous, adversaries are diversifying and adopting more strategic and multi-stage tactics. They've identified that factors such as high financial and regulatory penalties and reputational damage offer more leverage to extort money from victims. As a result, it is now easier than ever for criminals with minimal skill to execute highly impactful attacks. Destructive attacks and the sale of direct access into corporate networks are also rising trends and the lucrative payoff potential from all these is changing how adversaries approach their craft.

For example, island-hopping attacks, a term used to describe the process of undermining a company's cyber defenses by going after its vulnerable partner network rather than launching a direct attack, have grown more common in recent years. They find the weakest link in a chain and use that to gain access to their real target (s), taking advantage of the trust that businesses have in each other. The Solarwinds attack is a powerful recent example. A threat actor was able to compromise the software company and inject a malicious payload into an upcoming software update. All Solarwinds clients whodownloaded that update were infected, which was thought to be around 100 US companies including Microsoft.

These threats won't dissipate any time soon. In fact, it is highly likely that cloud-jacking through public clouds will become the island-hopping strategy of choice for cybercriminals as opportunity proliferates due to the overreliance on public clouds by the distributed workforce.

This means that security around remote working will continue to be on the agenda of many organizations, especially with the increasing number of unprotected endpoints, leading to an enlarged attack surface. This will undoubtedly lead to increased business email compromise attempts and attacks against VPNs and other remote working infrastructure.

Cloud adoption will accelerate even further with many organizations looking to the cloud earlier than they had planned. Remote working is here to stay.IT teams are still adjusting into these newer ways of working, which necessitates increased training for staff on how to operate securely when working remotely.

A Fortra survey, whereby 250 CISOs and CIOs from financial institutions were surveyed around the cybersecurity challenges they face, found that nearly half (46%) said cybersecurity weaknesses in the supply chain had the biggest potential to cause the most damage in the next 12 months.

What Sectors Are More at Risk?

The very nature of an interconnected supply chain means that no sector is safe from this threat. But there are some that are more exposed than others. Those that are particularly vulnerable operate within critical vertical sectors such as Financial Services (FS), defense, healthcare, and public sector organizations. Not only do they carry valuable personally identifiable information (PII) and sensitive data, but they also have very large supplier ecosystems, meaning the threat can potentially go much further.

Financial Services

FS is a sector that has long been a key target for cyber-attacks, and hackers are rejecting frontal assaults on well-defended walls in favor of infiltrating networks via vulnerabilities in suppliers. This means every blind spot in the supplier ecosystem is highly likely to be obscuring cyber threats. Likewise, increasing operational flexibility, through the deployment of cloud infrastructure, for example, is critical for future FS competitiveness, but it has also driven regulatory evolution around the use of third-party suppliers, in what was already a highly regulated sector.

The Security and Exchange Commission's Office of Compliance Inspections and Examinations listed supplier management as a key area in its best practice guidance for regulated companies, underlining that this is a topic of growing focus for regulators.

Add to this the growth in regulation, such as CCPA, GDPR and other global privacy legislation, and it is understandable why compliance is a key driver for managing cybersecurity risk in the supply chain.

Healthcare and Pharmaceutical

There's an obvious, increasing focus on security in healthcare and pharmaceutical, with many organizations witnessing a huge uptick in attacks as precious intellectual property (IP) is targeted. This reflects criminal cyber-attack groups continuing to target industries where there are huge financial rewards, as well as nation states attempting to steal IP; in healthcare this was driven by the COVID-19 pandemic, and the many worldwide vaccine initiatives and trials. This momentum has been maintained. In fact, vaccine-related data pertaining to trials and formulae is some of the most sought-after IP and the drive to get hold of it for financial or political gain is putting healthcare and pharmaceutical organizations under intense pressure.

Vaccine-related data pertaining to trials and formulae is some of the most sought-after intellectual property.The European Medicines Agency, which assesses medicines and vaccines for the EU, was victim of a targeted cyber-attack in which documents related to the development of the Pfizer/Biontech vaccine were accessed.

At the same time the healthcare sector will see the adaptations it made to try and maintain patient services become a vulnerability. With growing reliance on telemedicine for routine medical appointments lucrative personally identifiable information (PII) is being accessed from remote locations and as a result is more easily intercepted by hackers. The dark web market for health-related PII and insurance data is booming. As a result, attackers are becoming increasingly creative about how they gain access to healthcare provider networks, employing island-hopping tactics that mean the larger the supplier ecosystem, the greater the associated risk.

Public Sector

Public sector organizations worldwide face a daunting set of challenges as society adjusts to a post-COVID-19 environment. Whether it is local government, social services, law enforcement or emergency services, organizations across all disciplines that depended on in-person processes were forced to pivot to digital alternatives at an uncomfortable speed. This rapid digitalization has opened a real window of opportunity for hackers. Not only do public sector organizations hold large amounts of PII, but the speed at which they had to transform has potentially left gaps in their cybersecurity. When you factor in the typically vast supplier ecosystems for most public sector organizations, it is easy to see why it's one of the vertical industries most at risk.

Defense

The defense sector is undergoing a transition away from proprietary technology solutions developed in-house towards buying commercial off-the-shelf solutions. This allows the sector to leverage the benefits of fast-paced development and competitively driven innovation. However, it also broadens and deepens the supplier base, creating greater exposure to third party risk which, in such a critical and confidential sector, must be closely managed to avoid threats to national security.

The defense sector is naturally a prime target for nation state-sponsored cyberattacks as geopolitical tension continues to rise in an uncertain global landscape. This has been illustrated by the Russian invasion of the Ukraine in Q1 2022. Not only has Russia mounted a series of cyberattacks against Ukraine, but there has also been a knock-on effect to the broader supply chain. One attack against communications firm Viaset had a primary target of the Ukrainian military, but many others affected. This included personal and commercial internet users, but also wind farms in central Europe.

Infosecurity Group's *2022 State of Cybersecurity Report* stated that nation-state attacks were the second biggest concern for European cybersecurity professionals. Defence was already a sector vulnerable to supply chain attacks, but recent events have only served to heighten that vulnerability.

Attacks against the supply chain can be very subtle, with cyber criminals infiltrating the vendor with malware or phishing emails and taking over accounts which they then use as a gateway to breach the larger organization, especially if there's already a trusted relationship between them.

An example of island-hopping: A utilities company suffered a data breach when cyber criminals targeted it via its law firm, compromising the account of someone at the firm and using that to compromise the utility company. By compromising the inbox of an employee, the attacker could exploit the identity of a real person and their real inbox, meaning the normal protections against phishing emails didn't work because it was an email from a trusted person – but unfortunately it wasn't the genuine contact, it was an attacker.

What Can Organizations do to Protect Their

Fully understanding the complexity of international supply chains is still proving to be a challenge. A McKinskey study with global supply chain leaders recently revealed that 45 percent of respondents either have no visibility into their upstream supply chain or can see only as far as their first-tier suppliers.

Clearly in today's market of disappearing perimeters between the organization and its partners, the threat of the extended supplier ecosystem is substantial. But with the sending and receiving of information essential for the supply chain to function – via email and other means - the only option is to better identify and manage the risks presented. The demand for greater resilience across supply chains over the next few years will require organizations to overhaul existing technology investments and prioritize cyber, email, and data security governance.

Carry Out Essential Due Diligence

At the very least, organizations should ensure that both they and their suppliers have the basic controls in place such as Cyber Essentials, NIST and ISO 27001, coupled with good data management controls.

Organizations need to thoroughly vet and monitor supply chain partners through audits, questionnaires, security ratings and other means. They need to understand what data partners will need access to and why, and ultimately what level of risk this poses. Likewise, they need to understand what controls suppliers have in place to safeguard data and protect against incoming and outgoing cyber threats. This needs to be monitored, logged, and regularly reviewed and a baseline of normal activities between the organization and the supplier should be established. This way the organization will be able to quickly detect unusual and/or malicious activity.

Invest in Cybersecurity Training for Employees

As well as effective processes, people also play a key role in helping to minimize risk. Cybersecurity training should be given so that employees are aware of the dangers and know how to spot when an email has been compromised or a URL is suspicious. Social-engineering emails can look incredible realistic and use topics that play on people's good natures, so their guard may be down for a moment. Knowing what to look out for in such an email is invaluable.

They should also be made aware of data regulation requirements and understand what data can be shared with whom. These requirements often change, so any training should be ongoing. And finally, they should also know exactly what to do in the event of a breach, so a detailed incident response plan should be shared and regularly reviewed. Training should be viewed as more than a one-off exercise, with regular updates and reminders —especially important with many employees working from home for at least part of their working week.

Use Technology to Secure and Defend

IT is essential for collaboration and communication, yet unpatched systems or poor password practices can leave an organization vulnerable. IT best practices should be applied to minimize these risks.

When IT is used effectively, it provides the last line of defense against cyber-attacks and can automatically protect sensitive data so that when employees inevitably make mistakes, technology is there to safeguard the organization.

Secure Data and File Transfers

So how do organizations transfer information between suppliers securely and how do they ensure that only authorized suppliers receive sensitive data?

Here Data Classification tools are critical to ensure that sensitive data is appropriately treated, stored, and disposed of during its lifetime in accordance with its importance to the organization. Through appropriate classification, using visual labelling and metadata application to emails and documents, this protects the organization from the risk of sensitive data being exposed to unauthorized organizations further down the line through the supply chain. The use of visual labels helps to educate users around how data should be handled before they go ahead and share it with a particular supplier.

Data that isn't properly encrypted in transit can be at risk of compromise, so using a secure and compliant mechanism for transferring data within the supply chain will significantly reduce risks. **Managed File Transfer (MFT)** software facilitates the automated sharing of data with suppliers. This secure channel provides a central platform for information exchanges and offers audit trails, user access controls, and other file transfer protections, including the removal of sensitive data, ransomware, malware, and other types of cyber threats from both outgoing and incoming data.

Defend Against Cyber Threats

Organizations should also layer security defenses to neutralize any threats that come in from a supply chain partner, for example a spear phishing email campaign. Due to its ubiquity, email is a particularly vulnerable communication channel and one that's often exploited by cyber criminals posing as a trusted supply chain partner. It's vital to have a solution that stops inbound spear phishing, business email compromise, and email account takeover attacks from even reaching employees. This protects customers and business partners from malicious email spoofs with automated DMARC email authentication. If an email does slip through, the risk can be mitigated, even engaging with cybercriminals to capture unique data and insights to outmanoeuvre threat actors.

It is also essential that organizations are adequately protected from incoming malware, embedded Advanced Persistent Threats, or any unwanted data received over email that could pose a risk to compliance.

Likewise, with such a high and growing dependency on cloud, organizations need to ensure that documents uploaded and downloaded from the web are also thoroughly analyzed, even if they are coming from a trusted source. To do this effectively, organizations need a solution that can remove risks from email, web and at endpoints, yet still allows the transfer of information to occur. Unlike traditional Data Loss Prevention (DLP) software solutions, Adaptive DLP does not take a 'stop and block' approach. Instead, it allows the flow of information to continue while removing threats, protecting critical data, and ensuring compliance. It doesn't become a barrier to business or impose a heavy management burden.

This is important because the traditional DLP 'stop and block' approach has often resulted in too many delays to legitimate business communications and high management overheads associated with false positives. This often leads to organizations watering their data security policies down, which exposes them to greater risk and a false sense of security.

An Adaptive DLP approach reduces these pain points, policies are enforced effectively, risks are removed, and data can be shared without disruption.

In Conclusion

The turbulence of the past two years has forced many organizations to address vulnerabilities in their globalized and complex supply chains. Any supply chain can have a number of vulnerabilities but one of the main targets will always be email. That's why a robust, scalable, and flexible email security system is a must-have for any enterprise seeking to minimize supply chain cybersecurity threat.

Whatever happens in the world from this point on from an economic, health and business perspective, managing risk in the supply chain is going to be a top priority. Where organizations have large supplier ecosystems the potential for cyber-attacks and data breach risks increases.

To combat this, organizations must put in place technologies to better protect the business so that they can gain visibility and control of their data, ensure email is not a weak point drive risk-reduction strategies across their supplier base. But they need to be confident that their data security tools and data protection policies are being enforced, in a way that minimizes business interruption.

According to the IBM 'Cost of a Data Breach 2022' report, the average cost of a data breach increased by 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022.

Ultimately, we recommend that any technology be applied in line with other defensive processes, and with training for employees to recognize cyber and data loss threats – in particular the phishing emails that look so realistic and can be so damaging - to fully minimize the risk. At the same time, organizations need to proactively drive supplier risk-reduction activity by building constructive support for suppliers into their cyber and data security programs. This includes alerting the supplier when new risks emerge and providing practical steps for them to follow to help solve the problem. At the end of the day if one of these suppliers mismanages customers' private data or suffers a cyber-attack, it is the organization's brand that suffers, and it is the company that owns the legal and regulatory risk – not the supplier.

Our data security suite allows organizations to communicate and collaborate securely, safe in the knowledge that none of their sensitive data is being inappropriately shared with suppliers.

Fortra Data Security

Today Fortra is an integral part of an organization's overall cybersecurity strategy and our email security suite is a comprehensive suite of best practice tools, all geared towards ensuring email is secure but uninterrupted. The suite allows organizations to understand their sensitive data and keep it secure throughout its lifecycle, no matter where that data resides and no matter how it is shared with partners. It comprises expert-curated threat intelligence, mitigation against brand impersonation, security awareness training, and data leakage protection, Fortra email security solutions safeguard organizations' digital assets and allows organizations to communicate and collaborate securely, safe in the knowledge that none of their sensitive data is being inappropriately shared with suppliers. This means they avoid costly damage to reputation and legal fines, while ensuring that these protections don't become a barrier to legitimate business processes or incur high management overheads

Our comprehensive data security suites include:

- **Data Classification**
  - Data classification is the foundation of a solid cybersecurity strategy. Sensitive data is identified, labelled, and controlled
- **Anti-Phishing**
  - With phishing such a dangerous threat, this industry-leading technology helps safeguard against advanced phishing and socially engineered email attacks through an intuitive cloud-based platform.
- **Adaptive Data Loss Prevention (DLP)**
  - Minimizes the risk of a data breach by automatically removing sensitive data from emails and documents as they are sent, received, or transferred to the cloud.
  - Adaptive DLP applies an additional layer of sanitization to protect from phishing, ransomware, and other Advanced Persistent Threats.
- **Digital Risk Protection**
  - Safeguard digital assets via expert-curated threat intelligence and complete mitigation against brand impersonation, data leakage, social media threats, account takeover, and other digital risks in one solution.
- **Secure Managed File Transfer (MFT)**
  - For sharing files without email, MFT provides a secure and compliant way to share data outside the organization.
  - Large file acceleration helps move that data quickly and securely

For more information, visit: https://www.fortra.com/solutions/cybersecurity/data-security

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.