GUIDE *(Cybersecurity)*

Managing Cybersecurity Risk in the Supply Chain

Supply Chains – Today's Fastest Growing Cybersecurity Threat

Business ecosystems have expanded over the years owing to the many benefits of diverse, interconnected supply chains, prompting 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 to have cybersecurity vulnerabilities to bring a business to its knees. To this point governments around the world have highlighted supply chains as an area for urgent attention in tackling cyber risk in the coming years. For example, in the UK, the National Cyber Security Centre has provided guidance around supply chain security proposing a series of 12 principles, designed to help organizations establish effective control and oversight of their supply chain.

This is because breaches originating in third parties are common and costly – a Ponemon Institute/IBM study found that breaches being caused by a third party was the top factor that amplified the cost of a breach, adding an average of $370,000 to the breach cost. Further, a BlueVoyant 2020 study into global supply chains found that 80% of organizations surveyed experienced a cybersecurity breach that originated from vulnerabilities in their supplier ecosystem and the average respondent's organization had been breached in this way 2.7 times.

Clearly supply chain cybersecurity threat is a growing challenge. This guide looks at how the attack surface has expanded as a result of COVID-19 and the impact that increased remote working will have 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 data security strategy.

Ponemon Institute reports that 53% of businesses had suffered a breach via a third party with $8 million being the average remediation cost from a third-party breach.

The 2021 Threat Landscape

Unfortunately, wherever there is disruption, cyber criminals see opportunity. Alongside the devastating health and economic impacts of the global coronavirus pandemic, there has also been a huge escalation in ransomware, phishing, and island-hopping attacks, as organizations shifted employees to working from home. Stretched security teams have been challenged to rapidly deploy robust remote working facilities to maintain productivity which has been a huge distraction, one that hasn't gone unnoticed by cyber criminals.

Attacks are not only more frequent, they are also more sophisticated as highlighted in the 2020 VMware Carbon Black Threat Report, as adversaries strive to maximize the revenue potential from each hit. 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. You only have to look at the well-publicized NotPetya attack a few years ago to see the devastation these tactics can cause.

As we move into 2021 these threats won't dissipate, and 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 newly distributed workforce.

In the 2017 NotPetya attack the servers of Ukrainian software company Linkos Group, vendors of accounting package M.E.Doc, were hacked and trojan software injected. This went on to infect M.E.Doc customers, ultimately crippling multinational companies from shipping giants Maersk to food producer Mondelēz and many more. At the time this attack was assumed to be highly sophisticated and a situation where the victims could have done little to prevent it. But that is not wholly true; the attack was bold, but not complex. Where the real danger emerged was in the fact that Linkos was simply not important enough in any of those large companies' hierarchy of suppliers to be the subject of security monitoring, it was overlooked.

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, following 2020's COVID-19-driven migration. Many organizations will be looking to the cloud earlier than they had planned. Remote working is here to stay, even after the pandemic, as part of a more hybrid approach to the workplace. IT teams are settling into this 'new normal' way of working as lockdowns come and go. This necessitates increased training for staff on how to operate securely when working remotely.

A recent HelpSystems 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. This was closely followed by increased working from home during COVID-19, which 36% of respondents selected as the threat with the potential to cause the most damage in the next 12 months.

What Sectors Are More at Risk?

In this expanded threat environment, all organizations are exposed to a degree of supply chain risk. Those that are particularly vulnerable operate within critical vertical sectors such as financial services, defense, healthcare, and public sector organizations – as they carry valuable personally identifiable information (PII) and sensitive data, while also having very large supplier ecosystems.

Financial Services

Financial services are a big 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 financial services 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 earlier this year 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 has been driven by the COVID-19 pandemic, and the many worldwide vaccine initiatives and trials. In fact, vaccine-related data pertaining to trials and formulae is some of the most sought-after intellectual property right now 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 right now. Recently, 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 the ongoing 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 have been forced to pivot to digital alternatives at an uncomfortable speed. In the space of a year society has transformed beyond recognition and digital-first is now an imperative. However, not only do public sector organizations handle a wealth of sensitive personally identifiable information, but as outlined above they typically have large supplier ecosystems and, in the rush to pivot to deliver online services that have traditionally been human-activated, this leaves a window of opportunity for hackers.

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 cyber-attacks as geopolitical tension continues to rise in an uncertain global landscape.

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 Ecosystems?

According to Accenture, 94% of Fortune 100 companies experienced supply chain disruptions from COVID-19, and as much as 40% of cyber threats now occur indirectly through the supply chain.

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, the only option is to better identify and manage the risks presented. The demand for greater resilience across supply chains in 2021 will require organizations to overhaul existing technology investments and prioritize cyber 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. They should be aware of data regulation requirements and understand what data can be shared with whom. 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 regularly updates and reminders especially important with many employees working from home.

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. Therefore, it is 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

Whatever happens in 2021 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 and 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 a Ponemon Institute/CyberGRX Report: "The Cost of Third-Party Cybersecurity Risk Management" Third-party breaches remain an expensive problem. Over 53% of respondents have experienced a third-party data breach in the past 2 years at an average cost of $7.5 million.

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, 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.

HelpSystems Data Security

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.

Today HelpSystems is an integral part of an organization's overall data security strategy and our data security suite allows organizations to understand their sensitive data and keep it secure throughout its lifecycle, no matter where that data resides – on-premise, in the cloud, in hybrid environments – and no matter how it is shared with partners.

The HelpSystems 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, which 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 data security strategy. Sensitive data is identified, labelled, and controlled
- 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
- Secure Managed File Transfer (MFT)
  - 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.helpsystems.com/solutions/cybersecurity/data-security

helpsystems

www.helpsystems.com

About HelpSystems

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