Mighty Guides

Sponsored by Trustwave®

8 Experts on Achieving Better Supply Chain Security

How Businesses Can Manage Supply Chain Cyber Risk and Increase Their Resilience

Table of Contents

Introduction 3

Foreword 4

Chapter One: The State of the Modern Supply Chain 7

Chapter Two: Elements of Supply Chain Cyber Risk 10

Chapter Three: The Top Five Supply Chain Resilience Challenges 14

Chapter Four: Achieving Better Supply Chain Security 20

Chapter Five: You Are a Supplier, Too 25

Chapter Six: How a Trusted Partner Can Help 27

Learn More About Our Experts 30

Introduction

Supply chain cyber risk is an increasingly pressing issue for organizations across the globe.

According to a recent survey by the analyst firm Gartner, 89 percent of companies experienced a supplier risk event in the past five years. In the wake of the 2021 SolarWinds and Apache Log4j cyber incidents, organizations have become increasingly aware of the risks associated with their supply chains. Worldwide supply chain disruptions associated with the COVID-19 pandemic have highlighted the importance of supply chain risk management even further.

Despite these warning signs, Gartner reported that companies' awareness of supply chain risk and plans to mitigate this risk are not yet mature. Most organizations have a large volume of suppliers, yet they're not always aware of who these suppliers are or what data or systems they have access to. Without visibility into their supply chains, companies cannot properly assess, let alone manage, their associated risks. And because many organizations still use legacy supply chain risk management approaches, they are unable to scale them to handle the increased volume of supply chain relationships.

This guide explores the state of the modern supply chain and highlights the key elements of supply chain cyber risk affecting organizations today. It also identifies the top five supply chain resilience challenges, provides four best practices for achieving better supply chain resilience, and explains how a trusted partner can help organizations become more resilient in less time.

All the best,
David Rogelberg
Editor,
Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Foreword

Inputs, processing, outputs, and constraints—these are the fundamental factors that every business must consider when architecting a supply chain operations reference model to ensure that it will deliver predictably high quality results.

The supply chain is rarely a simple, single chain. With every vendor having vendors of their own, a security breach could truly come from any direction. And, as we all know, the supply chain is a hot target for cyberattacks. There's no avoiding it. While adversaries are evolving to find sophisticated, agile attack tactics, we cannot simply continue with the same security strategies we've always used or take the approach of "I'll just make sure I use only secure vendors." It takes a comprehensive, proactive approach to truly begin to secure against threats.

In this guide, we explore the topic of supply chain security with an approach that's several layers deep. Not only should organizations be treating suppliers like they're part of the organization when it comes to security and transparency, but that same standard needs to be upheld for their suppliers and beyond. We've interviewed eight industry experts worldwide for their expertise on what, exactly, a mature supply chain security posture looks like. I hope you'll leverage their collective insight to view your security with a fresh perspective.

Regards,
Kory Daniels
CISO,
Trustwave

Trustwave®

As a recognized global cyber defender that stops cyber threats all day, every day – we enable our clients to conduct their business securely.

Trustwave detects threats that others can't see, enabling us to respond quickly and protect our clients from the devastating impact of cyberattacks. We leverage our world-class team of security consultants, threat hunters and researchers, and our market-leading security operations platform, to relentlessly identify and isolate threats with the right telemetry at the right time for the right response.

Trustwave is a leader in managed detection and response (MDR), managed security services (MSS), consulting and professional services, database security, and email security. Our elite Trustwave SpiderLabs team provides award-winning threat research and intelligence, which is infused into Trustwave services and products to fortify cyber resilience in the age of advanced threats.

Trustwave®

MANAGED DETECTION
AND RESPONSE

Be the Hunter, Not the Prey.

BEGIN THE HUNT

Meet Our Experts

Nick Ellsmore
SVP, Worldwide Consulting and Professional Services, Trustwave

Ali Ansari
Managing Director, Taulia

Matthew Otwell
CISO, Maryland Department of Health

Steven Parker
CISO, TBC Corporation

Kevin Tham
CISO, Avenue Bank

Olga Voytenko
Managing Director, State Street

Terry Wasti
Director Infor FSM Supply Chain, Grant Thornton LLP

Tyrone Watson-Ferguson
SVP/CISO, Security Bank of Kansas City

Chapter One

The State of the Modern Supply Chain

Although thinking of the supply chain as a single issue or entity may seem intuitive, the reality is much more complex, with multiple layers of complex vendor relationships branching out extensively. When considering how to manage supply chain risk, organizations may find it more helpful to envision the supply chain not as a single chain but as a supplier network or supplier ecosystem—in part because many businesses, without even realizing, have greatly expanded their supply chain relationships over the past several decades, particularly in recent years.

How did this expansion take place? For a variety of reasons, organizations often choose to outsource and offshore a large portion of their operations, massively increasing the total number of suppliers they must manage—sometimes tens of thousands. The problem is compounded when companies are involved in a merger or an acquisition, as they likely will add to their ranks additional suppliers who then must also be managed.

Shadow information technology (IT)—in which employees sign up for external IT systems, devices, software, applications, and services without corporate approval—has also accelerated, bypassing the traditional security checkpoint organizations use to assess supplier risk and obscuring the full scope of suppliers from the organization's view. Lastly, legacy vendor risk management systems originally designed for paper-based workflows have not successfully scaled to meet the increased volume of supplier relationships, making supplier risk even more difficult for companies to manage.

"Supply chain is a colloquialism for supply network or supply ecosystem. They all describe a system of inputs used to create outputs."

Tyrone Watson-Ferguson
SVP/CISO,
Security Bank of Kansas City

As the supply chain ecosystem has become steadily more complex, recent events unrelated to cybersecurity—such as supply chain disruptions arising from the COVID-19 pandemic—have demonstrated that businesses must urgently find effective strategies for managing their supply chain risk, or else they jeopardize their ability to serve their customers. Meanwhile, supply chain security breaches have significantly increased; the media regularly covers supply chain cyber incidents resulting in data breaches.

> **Supply chain is the right umbrella term for the problem, but solutions have to be designed for its individual components.**

Nick Ellsmore
Senior Vice President,
Worldwide Consulting and Professional Services, Trustwave

The Apache Log4j vulnerability brought the issue of software supply chain security to the forefront in December 2021, when a series of critical vulnerabilities were disclosed and attacks soared in their wake. The SolarWinds hack, which came to light earlier that same year, highlighted how a nation-state actor could compromise hundreds or even thousands of organizations simply by compromising the provider of their IT monitoring tools.

This type of supplier breach has become more commonplace in recent years. Faced with a broad range of threats, companies must understand all the elements of supply chain cyber risk, identify which types of risk apply to them, and develop strategies for managing these risks.

"Many companies run business processes through technology solutions/ platforms which are often provided by a technology supplier. An interruption in those suppliers can have a serious impact on a company's operations."

Kevin Tham
CISO,
Avenue Bank

Key Points

- The supply chain is better described as a supplier network or supplier ecosystem than as a single chain.
- Businesses now have vast numbers of suppliers to manage, and they often don't know exactly who all their suppliers are.
- Recent cyberattacks have targeted the supply chain itself, resulting in mainstream breaches that have made effective management of supply chain cyber risk an urgent priority.

"In the past, supply chain was a linear concept—one way in and one way out. Now a supply chain sees multiple points of ingress and egress, and supply chain management encompasses design, planning, execution, control, and monitoring of its activities to ensure goods and services are delivered."

Matthew Otwell

CISO,
Maryland Department of Health

Elements of Supply Chain Cyber Risk

As previously noted, supply chain risk spans a broader range of categories than one might first assume. An organization's list of suppliers is stunningly wide ranging. This list can span from office cleaners (who likely have access to documents left on employees' desks) to hyperscale cloud service providers holding all of a company's data.

> **Assess the risks your company faces with regard to geopolitical risk, technology compromise risk, and supplier breach risk, and manage them accordingly.**

Nick Ellsmore
Senior Vice President,
Worldwide Consulting and Professional Services, Trustwave

The manufacturer of every piece of computing and connected hardware used in an organization is a supplier—including the companies that made any device employees brought in without informing their IT department. The risk exposure associated with each of these suppliers varies enormously, and different approaches are needed to manage the respective risk involved.

"Cyber risks, like geopolitical risk, technology compromise risk, and supplier risk, negatively affect the quality and availability of materials companies need to build their products and conduct operations safely and effectively."

Tyrone Watson-Ferguson
SVP/CISO,
Security Bank of Kansas City

Organizations typically face one or more of the following risk scenarios:

- Geopolitical risk
- Technology compromise risk
- Supplier breach risk

Geopolitical risk

This risk category applies primarily to nations, governments, and organizations with a plausible chance of being targeted by nation-state attackers.

An uptick has occurred in the number of cyberattacks conducted by nation-state-supported threat actors, many with geopolitical motives. Though most organizations are more likely to be collateral damage than a target in these types of attacks—a risk profile which changes how these organizations should proactively prepare for such attacks—legitimate concerns about data integrity and trust arise in their wake. If you rely on suppliers or technology originating in a jurisdiction where nation-state interference could emerge, assessing the risk involved is essential. You should also understand the very limited response avenues available to you signing an agreement with a new supplier.

Technology compromise risk

This risk category affects all companies. The SolarWinds and Log4j vulnerabilities are prime examples.

The SolarWinds breach brought to light the exponential impact of a single vulnerability. While SolarWinds is an extreme example because of the intent behind the attack and the way the attack was executed, the reality is that the entire software industry lives within an ongoing cycle of vulnerability assessment and patching.

"As the world has transitioned to a global economy, supply chains have become more and more interconnected. Even within defense industries, it is common for one country to need parts from foreign suppliers. This poses a major geopolitical risk."

Terry Wasti

Director Infor FSM Supply Chain, Grant Thornton LLP

This cycle is not going to change. How you evolve your approach toward a resilience mindset—with an increased focus on early detection and rapid response—is key.

Supplier breach risk

This category of risk can apply to suppliers in three different ways:

- *Suppliers accessing your data*
- *Suppliers accessing your systems*
- *Suppliers critical to delivering your services*

Some supplier attacks, such as ransomware, can restrict access to networks and disrupt service delivery. Supplier breach risk can be mitigated through supplier diversification; if one supplier affecting fulfillment is down, another can step in and help offset the impact. Breaches that provide access to your environment or ultimately compromise your data residing with an impacted third-party supplier—like the many law firms and financial institutions targeted for customer data—require a more rigorous response.

"In prior years, malicious actors and ransomware gangs were focused on grabbing an organization's data. But now they've realized that by simply causing a disruption, an organization may have more incentive to pay the demands and get operations back to normal as quickly as possible."

Matthew Otwell

CISO,
Maryland Department of Health

Key Points

- Your supplier network is broader than you may realize.
- Supply chain risks generally fall into three categories: geopolitical risk, technology compromise risk, and supplier breach risk.
- You will need different supply chain risk management approaches for each of these risks, depending on the ones your company faces.

“Companies need to ensure data integrity throughout the supply chain. Security measures should ensure that all data states are secure when at rest and in motion. Risks range from supply interruptions to environmental and safety crises to information security breaches.”

Steven Parker

CISO,
TBC Corporation

Chapter Three

The Top Five Supply Chain Resilience Challenges

As you grapple with supply chain cyber risk scenarios that may apply to your organization, you may also run into obstacles preventing you from improving your supply chain resilience.

Here are five of the supply chain resilience challenges your organization is most likely to encounter and the ways they could affect your business.

1. Not knowing all your suppliers

For decades, organizations have adopted a management theory focused on specialization and core competency. As a result, they have outsourced, offshored, and otherwise separated all noncore operations from the business. While good for business, this separation greatly complicated the supply chain.

Organizations have thousands and, in some cases, tens of thousands of suppliers. Most of these suppliers are not formally considered IT service providers; however, they almost certainly have supply chain risk relevance at some level. Procurement teams have often not maintained comprehensive records of such suppliers, and mergers and acquisitions over the years have rendered many existing records inaccurate.

For these reasons, organizations usually cannot definitively list all their suppliers, let alone outline what they do or evaluate their cyber risk relevance. **It is self-evident to say that you cannot secure what you don't know is there**.

"The definition of 'supply chain' was introduced to explain an otherwise complex web of interdependencies that an organization faces. However, the term is far oversimplified. The industry has already moved on from talking about third parties to fourth and fifth parties."

Kevin Tham

CISO,
Avenue Bank

2. Treating supply chain resilience as a single issue

Just as the supply chain is not a single entity, supply chain resilience is not a single issue. Supply chain risk has many elements, and each one requires a different approach to risk management.

When dealing with software, hardware, and other components, you should start with an awareness of the technology supply chain, which branches out with not only your vendors but also their vendors, and beyond. You cannot simply say, "I'll assess my vendors," because it's not always just the parties you interact with but also the parties they interact with, fanning out several levels deep. Often, organizations don't realize they're using certain software. Without knowing what they're using, organizations cannot create a comprehensive awareness of their technology supply chain.

> **Most organizations don't understand who their suppliers are. A common reason for this lack of understanding is that mergers and acquisitions often occur over time.**

Nick Ellsmore
Senior Vice President,
Worldwide Consulting and Professional Services, Trustwave

For example, assume your car has one small bolt crucial to the car's safe operation. Without this bolt, the brakes will not work. Software supply chain security is similar: One small software package may be buried deep in a system, but if this package is exploited, the entire company may be impacted. Taking this concept one step further, suppose a third party manufactured the bolt. You don't know the quality of steel used to manufacture that bolt.

"While a hired third party may be able to withstand disruption and operational challenges, their sub-processors or third-party suppliers may lack continuity capabilities. Transparency into the Nth party within a supply chain supports resilience during times of stress."

Olga Voytenko
Managing Director,
Global Head of Risk Management,
State Street

Cars are made of hundreds of components supplied by hundreds of specialist providers. If you assess only the car manufacturer or its direct suppliers, you could easily miss an issue with one of the subproviders. On the other hand, assessing all subproviders is impractical for most organizations.

In such a scenario, you may be able to find a suitable middle ground by assessing the management system and supply chain risk management processes in place by the car manufacturer. These elements are complex, interrelated, and require a fit-for-purpose risk management solution.

3. Relying on legacy systems that don't scale or provide useful data

Because most organizations' supply chain risk management processes evolved over time, possibly starting from a blank sheet of paper, they are likely still manual. In most cases, the organization emails out an Excel spreadsheet of questions to a vendor, assesses the vendor's responses, and forms a view of the risk involved. Maybe the results are stored centrally in a register or system, or maybe they're stored in a paper file system. Or maybe they are not properly stored at all.

> **When different organizations come together, they don't have the luxury of a single central system that has accrued suppliers' information.**

Nick Ellsmore
Senior Vice President,
Worldwide Consulting and Professional Services, Trustwave

"As an industry, we have spent the last 10 years shifting procurement and contract processes to include third-party supplier due diligence. However, this process now needs to be extended to fourth- and fifth-party suppliers, which most solutions will not scale for, both from a structural perspective and from a commercial perspective."

Kevin Tham
CISO,
Avenue Bank

These legacy systems don't scale, and they don't provide the basis for usable aggregated reporting. At the same time, organizations must now address much larger volumes of vendors than ever before, and so traditional manual systems are beginning to buckle. Having the right systems, tools, and automation in place is critical to keeping your supply chain risk management processes running efficiently and accessing actionable data insights for managing risk.

4. Treating suppliers as the enemy

The supply chain risk management process is frequently unilateral. The message organizations frequently send, whether intentionally or not, is, "We are the customer, and you will give us the information we demand or we will not do business with you." This adversarial approach does not engender a strong relationship between customer and supplier, and, ultimately, the strength of this relationship determines whether information flows freely between the two parties.

And, of course, almost every company is both a customer to its suppliers and a supplier to its own customers. Trust goes both ways. Being reasonable, collaborative, and supportive in working with your suppliers simply makes sense.

5. Lacking sufficient cybersecurity staffing and skills

Cybersecurity is a fascinating business. Every day, new challenges arise. Cybersecurity professionals are attracted to exciting, dynamic roles in which they take on interesting work and perhaps have their pick of job opportunities.

"The culture of an organization plays a major role regarding the success or failure of change. Slow adaptation to fortifying supply network security poses increased risk, as malicious actors are taking advantage of security gaps."

Matthew Otwell

CISO,
Maryland Department of Health

Business leaders, particularly those serving in technology and security roles, widely acknowledge that cybersecurity suffers from an industry-wide skills shortage. According to the 2021 (ISC)² Cybersecurity Workforce Study, the global cybersecurity workforce needs to grow by 65 percent to effectively defend organizations' critical assets. Two-thirds (60 percent) of the study participants reported that a cybersecurity staffing shortage is placing their organizations at risk.

With these statistics in mind, consider how you are helping your cybersecurity professionals develop their careers. After all, the skills shortage means there is no lack of opportunities for a skilled cybersecurity practitioner. If these professionals are not kept interested in their work, they may well walk, leaving the organization to fill even more roles.

"A company's supply chain exposes it to factors that are outside of its control. Therefore, it's essential to understand how relationships with other companies affect one's own business and make the right decisions about which organizations to partner with."

Ali Ansari

Managing Director,
Supply Chain and Payables Finance,
Taulia

Key Points

- To understand your technology supply chain, look not only at your vendors but also at their vendors, and beyond. Look several levels deep.
- Legacy supply chain risk management processes don't scale, and they don't provide for usable aggregated reporting.
- An adversarial approach to supply chain risk management places companies and suppliers in a difficult position to build the trust necessary for transparency and information sharing.

"Interconnected systems, processes, and resources have created a complex supply matrix rather than what we view as the legacy supply chain."

Kevin Tham

CISO,
Avenue Bank

Chapter Four

Achieving Better Supply Chain Security

Given the complexity of today's supply chain landscape and the numerous challenges organizations face in becoming resilient, knowing where to begin improving your supply chain security may be difficult. These four best practices for supply chain cyber risk management will help you make meaningful progress toward this goal.

1. Understand who your suppliers are, what data they hold, what access they have, and what their criticality is to your business operations

Before you can roll out a supply chain security program of any type, you need to know the parties that make up your supply chain. Your procurement team will generally have a list of your suppliers as a starting point, but this list is almost certainly incomplete.

Shadow IT—particularly cloud services engaged directly by business units without procurement's involvement—can often be identified through analysis of corporate credit cards. Even so, the best move is putting an amnesty policy in place whereby employees across the business can share the third-party companies and services they've engaged with, without fear of repercussion.

"Due diligence is important for understanding the residual risk posed by your suppliers. The due diligence performed may identify control gaps overlooked through informal discussion with your supplier."

Olga Voytenko

Managing Director,
Global Head of Risk Management,
State Street

For each supplier, know three critical aspects:

- **Data:** The sensitivity and volume of data they hold
- **Access:** The network access and user credentials (particularly privileged credentials) they have
- **Criticality:** Their criticality to business operations (for example, a trucking firm may have little to no data and little to no access, but if the firm is shut down by a ransomware attack, you may no longer be able to run your business)

When assessing these aspects, ensure that the organization is enforcing the concept of **least privilege**—that is, vendors only have the access they need to effectively do their job, and the vendor's software is doing only what it is supposed to do, with minimal access rights.

> **We're still relatively immature at understanding and accepting that risk is not bad. Risk is just something to be managed.**
>
> 
>
> **Nick Ellsmore**
> Senior Vice President,
> Worldwide Consulting and Professional Services, Trustwave

2. Assess the security maturity of suppliers and ensure it lines up with their potential risk to your supply chain

Given the three critical aspects detailed above—data, access, and criticality—each supplier will present some level of risk to your organization. The higher the risk, the higher the level of security maturity you should look to be in place. As we'll explain in the next section, the ultimate goal should be to bring your suppliers into your security program.

"Cybersecurity is not just about defense anymore—it's about resiliency. Having a good data backup strategy, incident response, and business continuity plan are important to carry an organization through an attack."

Matthew Otwell

CISO,
Maryland Department of Health

For this reason, we don't recommend simply excluding suppliers deemed not mature enough when you first assess them. If they are the right business for you to work with and you're confident they can raise their security to the appropriate level, then there is nothing wrong with embarking on that journey with them.

The process of assessing a supplier's security maturity generally involves the following steps:

- Sending out a request for information (historically, this request has been conducted through an Excel spreadsheet or Word document; now, it's generally handled through a software as a service, or SaaS, application)
- Receiving and reviewing the responses
- Receiving and reviewing various points of evidence and supporting material—such as the International Organization for Standardization (ISO) 27001 Statement of Applicability/Certifications, penetration testing reports, and Service Organization Controls (SOC) 2 reports
- Clarifying information with the vendor, as necessary
- Formalizing the assessment into a report or consistent structure that allows for comparison between companies and over time

Note that this process isn't meant to be a pass/fail type of exercise. You want to understand how the supplier's controls line up with the risk related to data, access, and criticality, and gain the information and insight needed to identify any vulnerabilities in the supplier's existing security program.

"More corporations are recognizing the significant impact supply chain disruptions can have on their operations and are implementing supply chain due diligence policies."

Ali Ansari

Managing Director,
Supply Chain and Payables Finance,
Taulia

3. Bring your suppliers into your security program

If one of your suppliers is breached and your data leaks, it's your data breach. Because your suppliers are ultimately part of your organization's overall security posture, you should bring them into your security program. Particularly, strategic partners need to genuinely operate within your security program. So, bring them in.

Here are a few steps that can help your strategic partners operate within your security program:

- Provide plug-in processes, such as for incident response or incident notification, that interconnect with your own
- Invite them to participate in tabletop exercises and scenario security planning
- Consider what data you can get from them to ingest into your security monitoring platform
- Bring them into the scope of a red team engagement targeting your organization

As you undertake these steps, ensure you're giving your suppliers the support, and, in many cases, the investment, necessary to achieve your security objectives.

4. Ensure detection and response capabilities extend to cover supplier breaches

For certain categories of supply chain risk, adequate threat detection and response are really your only control. If a nation state tampers with the firmware of a technology product in your environment, it will not show up in a questionnaire sent to the technology vendor. You will only pick up the tampering through effective monitoring and detection technology, along with proactive threat hunting, which will identify behavioral anomalies and hidden breaches.

"Not enough attention is paid to supply lines. Working in the medical supply chain space, I see medical product supplies with out-of-stock issues all the time. This has huge downstream consequences."

Terry Wasti

Director Infor FSM Supply Chain, Grant Thornton LLP

Key Points

- To achieve better supply chain security, you will need to know what data your suppliers hold, the access they have, and their criticality to your business operations.
- Once you have this information, assess each supplier's maturity to ensure it is commensurate with the potential risk the supplier poses to your organization's supply chain.
- As you undertake these processes, consider bringing your suppliers into your security program.

"Due diligence is an important first step when engaging with a supplier. First and foremost, it provides a view on the supplier's attitude to security—whether they have the right security management systems and processes in place."

Kevin Tham

CISO,
Avenue Bank

Chapter Five

You Are a Supplier, Too

Supply chain risk management goes both ways. For this reason, "Do unto others as you would have them do unto you" is an important maxim to keep in mind when you're looking at supply chain security. If you're going to send out a 90-page questionnaire to your suppliers, then you should expect your customers will similarly send a 90-page questionnaire to you. Historically, organizations haven't invested in systems that make life easier for their suppliers. However, by giving suppliers the tools to make this process as simple and effective as possible, you can ensure everyone gets what they need to carry out their supply chain risk evaluations.

> **An online system will often allow for answers to be stored, reused, and prefilled. It also gives organizations better data on their suppliers.**
>
> 
>
> **Nick Ellsmore**
> Senior Vice President,
> Worldwide Consulting and Professional Services, Trustwave

Mature suppliers have already realized that this practice is in their best interest. These suppliers are building out self-service tools such as trust sites—for example, trust.atlassian.com and trust.salesforce.com—that make key compliance, security, and other assurance resources available on demand. A buyer can review these resources, assess the supplier's security state, and determine how the supplier's security program can connect into their own. The supplier benefits, too. Rather than wasting time answering the same questions and repeatedly fulfilling the same requests, they can simply direct buyers to a complete library of current self-help resources.

"Tools like third-party risk assessments and trusted sites promote continuous cybersecurity improvement within a supply network. They encourage workers and managers across silos and companies to identify, communicate about, and remedy problems."

Steven Parker
CISO,
TBC Corporation

Key Points

- Supply chain risk management goes both ways. Just as you need to evaluate your suppliers, your buyers need to evaluate you.
- Historically, organizations haven't invested in tools to make their suppliers' lives easier.
- Mature suppliers are building out trust sites and other self-service tools, which make the supply chain risk management process more efficient for everyone involved.

"Supporting documentation collected during due diligence when onboarding a vendor can inform a company about how to make the most of the vendor's security controls."

Olga Voytenko

Managing Director,
Global Head of Risk Management,
State Street

Chapter Six

How a Trusted Partner Can Help

Risk can't be eliminated, but it can be managed. You may never be able to gain 100 percent visibility into your supply chain, but better supply chain security is achievable. With this reality in mind, don't try to be perfect; instead, try to be better. To get to your desired end state, you should prioritize your security efforts. First, determine the most critical aspect to address. This approach allows you to properly direct your time, energy, and investment.

You may need some help implementing these best practices, especially if you're already juggling multiple high-priority initiatives. Identifying all your suppliers can take several months, and a proper evaluation can take a year or longer. A trusted partner can help you accelerate the process, providing the advanced tools, best practices, and experts needed to help achieve your supply chain risk management in less time. For example, Trustwave's service can streamline your supply chain risk assessment by consistently gathering critical data based on industry frameworks, identifying high-risk suppliers, and highlighting suppliers' security gaps.

In some cases, like geopolitical risks or technology compromise risks, fully vetting every single layer of your supplier relationships may not be practical or cost-effective. This common business challenge is why managed detection and response (MDR) is a key component of any security plan. An MDR partner levels the playing field for smaller firms or those without a large security budget. With an MDR partner, these organizations can proactively search for emerging threats, monitor risk to protect themselves, and respond quickly if a threat is identified. Trustwave's Fusion platform accomplishes these tasks by augmenting a client's existing security tools with advanced analytics and best-in-class Trustwave SpiderLabs threat intelligence and expertise.

"To ensure resilience, organizations need to invest in their supply chain management. The digitization of supply chain practices will improve visibility across the entire supply chain and help inform decision-making, forecasting, and proactive reallocation of resources."

Ali Ansari

Managing Director,
Supply Chain and Payables Finance,
Taulia

If needed, a trusted partner should have available the comprehensive resources for elevating your supply chain risk management program across the board. For example, Trustwave Security Colony offers a full library of resources developed for real clients, saving you the trouble and cost of reinventing the wheel. This service also includes a vendor risk assessment tool that proactively alerts you to your supply chain vulnerabilities, and a maturity assessment that precisely shows your current maturity level and how to advance to the next stage of maturity.

> **Supply chain risk management is a repeatable process, so it is actually much easier for an external partner to take on that type of high-volume task.**

Nick Ellsmore
Senior Vice President,
Worldwide Consulting and Professional Services, Trustwave

Supply chain risk management has never been more urgent or challenging, but the good news is that there are effective tools and best practices to streamline the process. An experienced partner can jumpstart your supply chain risk management program, giving you a roadmap to follow, and the right combination of people, processes, and technology to get to your destination. This way, your company can confidently manage the risks associated with today's increasingly complex and multilayered supply chain environment.

"Hackers know that a third-party vendor likely has access to the company's sensitive data. A single attack can impact a business's reputation and result in significant loss. A company should always be working to mature its supply chain risk management."

Steven Parker
CISO,
TBC Corporation

Key Points

- Identifying and assessing your supply chain risk can take a year or longer.
- A trusted partner can accelerate the process, leveraging tools and best practices on your behalf.

“Though it can be hard to see how the sums of supply chains create the final product, that network exists and needs to be protected.”

Tyrone Watson-Ferguson

SVP/CISO,
Security Bank of Kansas City

Learn More About Our Experts

Nick Ellsmore, Senior Vice President, Worldwide Consulting and Professional Services

Nick Ellsmore is an experienced cybersecurity entrepreneur who has built, merged, acquired, and sold multiple cybersecurity businesses. With over 20 years of experience in the industry, focusing on consulting and professional services strategies, information systems, penetration testing, and incident response, Nick is well known for bringing a highly collaborative, pragmatic perspective to the cybersecurity industry.

Ali Ansari, Managing Director, Supply Chain and Payables Finance, Taulia

Ali Ansari is a trade and supply chain finance professional with 25 years of on-ground experience in managing large businesses, leading innovation, and managing risk. He has worked in Europe, Asia and Africa with top tier multinationals including PWC, J.P. Morgan, BAML, HSBC and ABN AMRO. Ali is currently the Managing Director of Supply Chain and Payables Finance at Taulia, a fintech that provides working capital solutions.

Matthew Otwell, CISO, Maryland Department of Health

Matthew Otwell has been an IT and Information Security professional working with multiple global organizations for over 25 years. He specializes in security program governance, risk, and compliance (GRC) across various organizational business units including Information Technology (IT) and Operation Technology (OT)/Industrial Control Systems (ICS). Currently, he serves as the CISO for the MD Department of Health overseeing the implementation of a new information security program.

Steven Parker, CISO, TBC Corporation

Steven Parker is an innovative, business focused, information security professional with 20 plus years' experience implementing information security programs from a risk-based perspective for a variety of verticals. He has served in executive and senior management positions, with responsibilities including strategy development and execution, strategy and tactical alignment, and risk and crisis management, and holds the following certifications: CISSP, C|CISO, CISA, CFE, and ITILv3.

Kevin Tham, CISO, Avenue Bank

Kevin is an Information Security veteran focused on non-intrusive security strategies and solutions for enterprises. With over 20 years of experience in the Information Security industry, Kevin began his career as a Security Researcher and academic in Queensland. His pivot into the private sector originally landed him as a Security Engineer, and he currently serves as the CISO for Avenue Bank.

Olga Voytenko, Managing Director, Global Head of Third Party and Outsourcing Risk Management, State Street

Olga Voytenko is a Managing Director, Global Head of Third Party and Outsourcing Risk Management. She is responsible for managing third-party risks arising from State Street's reliance on outsourcing. These include risks related to ineffective third-party selection and failure to oversee and monitor third-party operations. Ms. Voytenko is responsible for building, deploying, and supporting the technology and processes to support business functions in mitigating third-party risks.

Terry Wasti, Director Infor FSM Supply Chain, Grant Thornton LLP

Terry Wasti is the Director of Infor FSM Supply Chain at Grant Thornton LLP. He is an experienced information technology leader with more than 25 years of experience helping organizations navigate complex supply chain solutions within the healthcare industry. Terry is responsible for the direction and strategy of the Infor Materials Management applications. His work includes architecture, assessments, design, transformation, training, implementations, and support.

Tyrone Watson-Ferguson, SVP/CISO, Security Bank of Kansas City

Tyrone Watson-Ferguson serves as Chief Information Security Officer for Security Bank of Kansas City. Tyrone has held many roles during his 25-year banking career and has served in Information Technology for the last 15 years.

Trustwave®

MANAGED DETECTION AND RESPONSE

Give Your Security Team More Venom

BITE BACK