MANAGING CYBER RISKS IN GLOBAL SUPPLY CHAINS: THE FOUR FUNDAMENTALS

APRIL 2020

HASLAM COLLEGE OF BUSINESS
THE UNIVERSITY OF TENNESSEE, KNOXVILLE

GLOBAL SUPPLY CHAIN INSTITUTE

Sponsored by leidos

NUMBER THREE IN THE SERIES TECHNOLOGY IN THE SUPPLY CHAIN

THE GLOBAL SUPPLY CHAIN INSTITUTE

WHITE PAPERS

GSCI has published several white paper series on topics such as technology, strategy, and innovation in the supply chain.

Our entire white paper library is available for download by going to the publications section at **gsci.utk.edu**

THE UNIVERSITY OF TENNESSEE KNOXVILLE

GLOBAL SUPPLY CHAIN INSTITUTE

MANAGING CYBER RISKS IN GLOBAL SUPPLY CHAINS: THE FOUR FUNDAMENTALS

THIRD IN THE **SUPPLY CHAIN TECHNOLOGY** SERIES
OF UT'S GLOBAL SUPPLY CHAIN INSTITUTE WHITE PAPERS

APRIL 2020

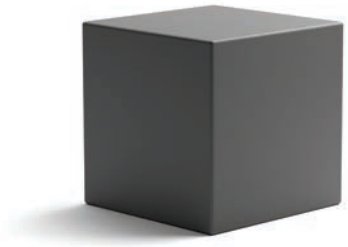
AUTHORS:
DAN PELLATHY, PhD
AYMAN OMAR, PhD

CONTRIBUTING EDITORS:
TED STANK, PhD
MIKE BURNETTE

THE UNIVERSITY OF TENNESSEE KNOXVILLE
GLOBAL SUPPLY CHAIN INSTITUTE

MANAGING CYBER RISKS IN GLOBAL SUPPLY CHAINS: THE FOUR FUNDAMENTALS

TABLE OF CONTENTS



Cybersecurity is currently one of the top challenges facing supply chain and business leaders.

Executive Summary

The Global Supply Chain Institute (GSCI) in the Haslam College of Business at the University of Tennessee, Knoxville, engages with dozens of business and supply chain leaders each year. All of these professionals communicate concerns about the business risks associated with cybersecurity. Cybersecurity is currently one of the top challenges facing supply chain and business leaders. The nature of cybersecurity creates a huge tension between working action plans to reduce risk versus action plans that increase efficiency through digital tools.

Over 30 companies and cyber experts were interviewed on the cybersecurity risks facing supply chains. These interviews provided a wealth of information on how supply chain professionals should understand and assess cyber risks to their organizations and what they need to be doing to build a cyber-secure supply chain. Out of these interviews, GSCI team formulated:

- Four fundamentals of managing cybersecurity
- Core definitions of fundamental aspects of cyber
- Key insights from examples of successes and failures

One key takeaway from our interviews was that the majority of supply chain leaders do not have a clear understanding of what they need to be doing to reduce cyber risk. Our experts reported that, all too often, supply chain professionals had an attitude of: “IT handles cyber” or “Everything must be fine as long as my PC is working.”

As we discuss below, a very different attitude exists in the companies that we interviewed that are leading the way in managing supply chain cyber risk. These benchmark companies recognize that cybersecurity needs to extend far beyond the four walls of their organization to their end-to-end supply chain. The leadership of these companies provide a clear cybersecurity strategy, and

These benchmark companies recognize

that cybersecurity needs to extend far beyond the four walls of their organization to their end-to-end supply chain.

then go to work building a cybersecurity culture to support their strategy. They also collaborate with supply chain partners when securing valuable supply chain assets to ensure that resources are invested for maximum impact. The key elements of these strategies mirror recent GSCI white papers in the "Supply Chain Strategy" series:

1. End-to-end
    - Over 60 percent of cybersecurity issues occur in third parties working in supply chains. How strong are the cybersecurity capabilities of 3PL and external manufacturing?
    - Supply chain cybersecurity is only as strong as the weakest link. How robust are the suppliers, contract manufacturers, and customers?
2. Integration
    - Risk increases at the interfaces. Does clear cybersecurity ownership exist in information and people systems linking suppliers, customers, external partners, internal supply chain disciplines, and business/supply chain interfaces?
3. Collaboration
    - Companies systematically misallocate dollars in cybersecurity if these investments are not made in collaboration with supply chain partners. Are different internal and external groups working closely together to solve problems and deliver common goals?
4. Total Involvement
    - Managing cybersecurity risk is not an IT job. It is the work of 100 percent of the organization across all business functions. Every person and information system creates risk.
    - Supply chain managers are trained to possess excellence in action planning, goal setting, problem solving, decision-making, and execution capabilities. Are cyber risks being managed by these skilled supply chain professionals?

This white paper provides supply chain leaders with strategic ideas, best practices, examples, and a fundamental management framework to reduce cybersecurity risk. This information can help shift you from an "unsure what to do" leader to a critical team member who is continuously working to mitigate cyber risk in the supply chain.

Introduction

Technology is probably the biggest –

but least well understood – threat to your supply chain..

Technology is probably the biggest – but least well understood – threat to your supply chain. Advances in information technology are allowing supply chains to drive efficiencies while also responding to fast-changing customer markets. At the same time, technological advances enable organizations to collect and make sense of massive amounts of data across a wide range of supply chain processes. The move toward digitalization, automation, and greater technological integration in the supply chain is not always pretty and is always complex. Our white paper entitled *"A SAVVY Guide to the Digital Supply Chain"* focuses on the need for a strategic approach to evaluating and leveraging technology to build a supply chain for the digital age.[i] That research suggests that supply chains, and the organizations that support them, are in the early stages of a digital transformation that will likely represent the biggest change to supply chain management over the next several years. At this point, the picture of exactly how things will look is still understandably blurry, but supply chain leaders must begin to incorporate this new paradigm into their strategies, plans, and organizations, or risk being quickly and irreversibly left behind.

The growing dependence on digital technologies, while in many ways necessary and beneficial, also exposes supply chains to cyber risks that can have a major impact on everything from operations to brand perception and consumer trust (supply chain tension). Perhaps the most important feature of these new cyber risks is that they can impact a business through the security weaknesses of partner organizations. To take just one example, in 2018, Marriott Hotels[ii] announced that cyber attackers had stolen contact information, passport numbers, credit card numbers, and other personal data on approximately 500 million customers. As events unfolded, it became clear that security systems at Marriott had not been breached directly, but that the attackers had penetrated Starwood Hotels, a brand that Marriott had acquired in 2016. This revelation meant that despite Marriott maintaining the security of their own systems, cyber attackers had nevertheless been able to steal customer data for years through a weakness at Starwood.

The Marriott example is just one of hundreds that are reported in the business press on a regular basis. Cyber risks arise from multiple sources. External actors may target company information, but people inside an organization who misuse company systems can also represent a serious threat. Moreover, the threats are

The growing dependence on digital technologies

while in many ways necessary and beneficial, also exposes supply chains to cyber risks

not only digital. There is a significant physical component to the cyber supply chain that includes servers and telecommunications devices people use to connect. Properly sourcing and maintaining this physical infrastructure is critical for cybersecurity. Globalization adds to the challenge: the physical components of a laptop or database might be produced in China or Japan while code that runs on these devices might be produced in Russian or India. Understanding these risks and having a strategy for managing them will be critical as organizations enter the uncharted territory of the emerging digital revolution.

Benchmark supply chain leaders focus on end-to-end integration to strengthen the weakest link in their supply chain and mitigate cyber risks

About This White Paper

The University of Tennessee's Global Supply Chain Institute (GSCI), in collaboration with industry leaders from across the supply chain management discipline, has produced a series of white papers on leading-edge issues in supply chain management. These white papers have covered topics from supply chain integration and collaboration to digitalization and platform management. In all of these white papers, we have provided professionals with practical "how to" guides and frameworks for managing critical aspects of the supply chain.

We interviewed over 30 senior supply chain executives

For this paper, we interviewed over 30 senior supply chain executives across numerous industries, from information technology companies, original equipment manufacturers, automotive suppliers, defense contractors, and supply chain consultants, to CPG, food, apparel, industrial, and consumer durables product companies. These senior executives manage truly global and complex supply chains, and all of them brought their extensive experience to our discussion of cyber risk. Additionally, to gain external perspectives, we interviewed a number of solution providers who are on the leading edge of supply chain cybersecurity.

Drawing from these interviews, and on discussions with managers from dozens of other companies with whom we have interacted through consulting and educational engagements, the research team developed four fundamentals for enhancing supply chain decision making on cyber risk. These fundamentals are concrete and implementable in any company. They can help managers raise awareness of cyber risks facing the supply chain and can also serve as guidelines to better position supply chains to meet these threats.

Cybersecurity Four Fundamentals

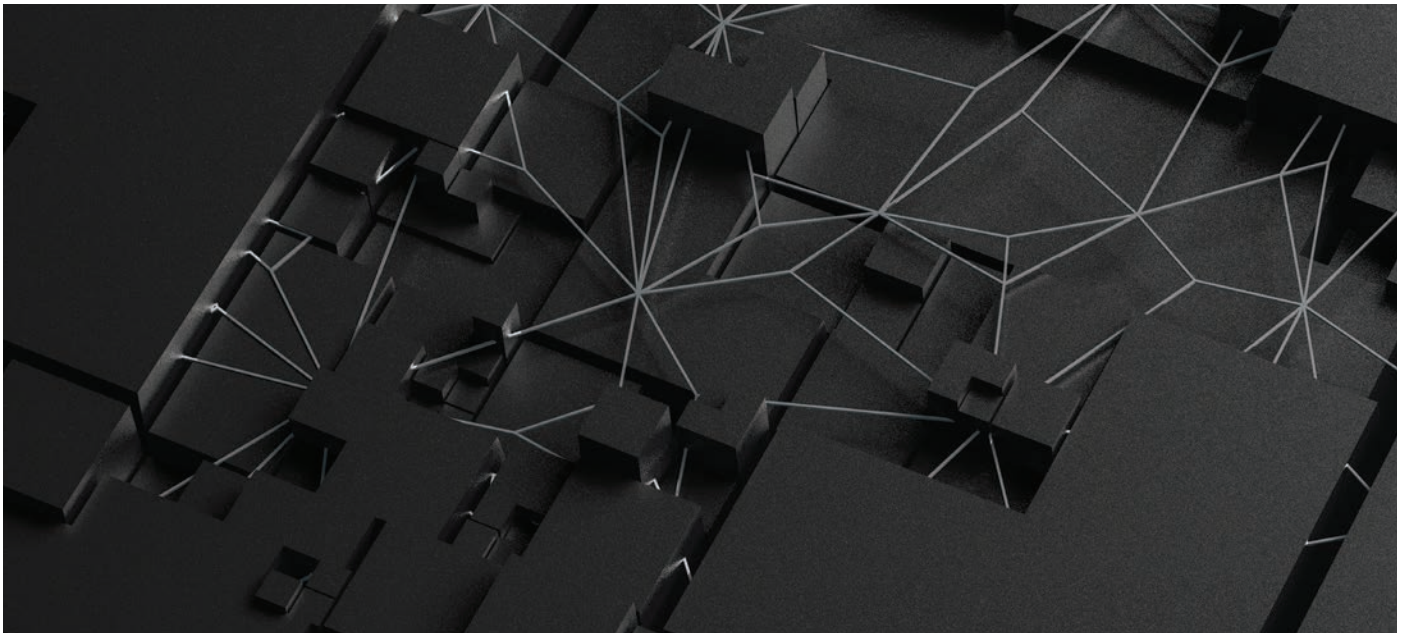
- Understanding the nature of cyber risks in the supply chain
- Developing a strategy and culture for managing cyber risks
- Integrating with key partners to manage cyber risks in the supply chain
- Deciding where (and how much) to invest in protecting the supply chain

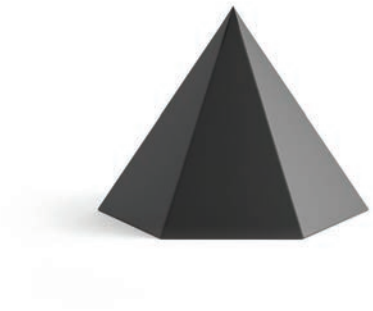
Cyber risk in the supply chain is a complex and evolving topic –

and no organization has it completely figured out.

These four fundamentals build on each other, supporting a holistic approach to cybersecurity in the supply chain. In discussing each of these fundamentals, we will examine specific examples of companies that have developed a clear understanding of the cyber risk and some of the leading-edge strategies they are using to counter these risks. These best-in-class companies have been on the forefront of cybersecurity issues – in some cases for decades – and worked with both private and governmental organizations in developing cyber risk mitigation capabilities in their supply chains.

Cyber risk in the supply chain is a complex and evolving topic – and no organization has it completely figured out. Despite these uncertainties, this white paper will give you concrete frameworks and examples that you can use in your organization to move the conversation forward.





Key Terms and Definitions

Supply chain professionals need to be focused on creating supply chains that deliver value today, while being positioned to meet the challenges of a digitalized tomorrow. But what does cybersecurity or cyber risk or a long list of frequently used terms even mean? How can these terms be used to drive understanding and action in an organization? Here are some key definitions required to understand cyber risk in the supply chain.

The prefix "cyber" is short for "cyberspace." Cyberspace is an environment in which a network of information technologies and human users interact. The "actors" within a cyberspace include[iii,iv]:

- Physical infrastructures and telecommunications devices that allow for connection to networks, such as SCADA devices (supervisory control and data acquisition, which are computer system used for gathering and analyzing real time data to monitor and control a plant or equipment), smartphones/tablets, computers, servers, etc.
- Computer systems and the related (sometimes embedded) software that creates operational functioning and connectivity
- Networks between computer systems
- Embedded processors and controllers
- Access nodes of users and intermediary routing nodes
- Constituent data, such as DNS (Domain Name Systems, servers that contain databases of public IP addresses and their associated hostnames used to resolve or translate those names to IP addresses as requested) records or data for the implementation of communication protocols
- And most importantly, people

Typically, the purpose of interacting in cyberspace is to create, store, modify, exchange, share, extract, and use information. The global internet is the best-known cyberspace environment, although "the cloud" and intranets also represent cyberspace environments. There are three key features of cyberspace that will be most relevant for our discussion in this paper: first, actors in cyberspace tend to be anonymous or difficult to identify; second, there tends to be a low cost for entering cyberspace environments; and third, the relationships between actors in cyberspace are characterized by asymmetric vulnerabilities

...the scope and nature of cyber risks

require systematic internal and external integration across stakeholders.

(for example, bypassing a system's strengths while targeting its vulnerabilities). "Cyber risk" is defined as "an operational risk to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" or "the risk involved with malicious electronic events that cause disruption of business and monetary loss." More broadly, the term cyber risk refers to multiple different risks within a cyberspace environment that can affect both digital and physical assets.

Cyber risks can be caused by internal or external vulnerabilities within a cyberspace environment. As discussed later in this paper, such risks can be classified by the source of the risk (e.g. malicious actors, external organizations, non-malicious actors); areas of vulnerability (e.g. points of weakness at external partners); or specific targets (e.g. information systems, electronic devices, unwitting individuals). Cyber risks can also arise out of mismanagement of information networks resulting in the loss of data and company intellectual property or a disruption in operations. This information-related aspect of cyber risk leads many people to use the term interchangeably with "information risk"; however, these terms are not entirely the same. Cyber risks encompass a much broader range of risks to both physical and digital assets.

A "cyber attacker" is an individual or entity perpetrating an attack. Cyber attackers are often a source of cyber risks, but not always. Simple mismanagement of information and related technologies can also present a source of cyber risk.

Finally, "cybersecurity" is the body of combined technologies, processes, and practices that are put in place to protect data, networks, and other digital and physical assets from attacks, damage, or unauthorized access.

Using this terminology we can start to discuss cyber risks in the context of today's global supply chains.

Benchmark supply chain leaders focus on end-to-end supply chain integration to mitigate cyber risks in the internal and external operating environment.

Seeing Cyber Risks in a Global Supply Chain Context

Supply chain cyber risks represent an emerging threat that organizations are only now starting to understand. One of the critical mistakes that organizations make is treating cyber risks like any other business risk. Traditional risk management models focus primarily on identification of, response to, and recovery from discrete events. Cyber risks, however, represent a constantly changing aspect of the broader digital environment. Cyber risk management, therefore, needs to be far more evolutionary, with continuous improvement of mitigation techniques as risks emerge.

One of the critical mistakes that organizations make

is treating cyber risks like any other business risk.

A health analogy is particularly apt. From a health perspective, viruses and other infectious agents are understood as simply a given part of the environment. Good hygiene is important to minimize the risk of infection but is not a guarantee against infection. To maintain health, the human immune system constantly responds and evolves in a complex interactive engagement with threats. Similarly, companies need not only "good hygiene" in terms of structures and investments that minimize cyber risks, but also a constant readjustment of their "immune system" in response to new threats.

But a lack of understanding about the sources of cyber risks and their potential impacts creates substantial challenges for organizations. First, it makes identifying vulnerabilities and predicting targets difficult. Attackers can be strategic attackers (i.e. target-focused), but perhaps more often they are not. A stray piece of open access code or a widget (e.g. www.quicksprout.com/top-10-widgets-to-improve-your-website) on a website might be a point of entry to company systems. Attackers might not have a clear target until gaining entry. This lack of clarity on the sources of cyber risk then makes it much more difficult to assign responsibility for defending the organization. Because organizations don't know how to characterize the threat, they throw responsibility for cybersecurity to the IT or legal department. As we discuss below, however, the scope and nature of cyber risks require systematic internal and external integration across stakeholders. Finally, because organizations are unsure of the target, they tend to focus on the obvious: customer data, intellectual property, loss of digital access. But breaches have implications that go far beyond lawsuits and loss of data.

...most supply chain managers are almost totally unaware

of where and how third-party risks may impact them.

The threat is real. The McAfee Center for Strategic and International Studies estimates that cyber crime costs the world economy about $445 billion annually. No wonder, then, that a survey of corporate leaders ranking business risks by Allianz Global Corporate and Specialty found that cyber risk has become the third most-important business risk. Cyber risks pose such a significant threat for the supply chain because they can have multiple cascading effects. The impact of a data breach can have a far-reaching influence on a company's reputation and its overall financial performance. As Yahoo was negotiating a buyout by Verizon, data breaches affecting billions of Yahoo users came to light. Although the acquisition eventually went through, the breaches led Verizon to downgrade Yahoo's valuation by $350 million.

Beyond data breaches, cyber incidents can cause major disruptions in the physical supply chain by shut down suppliers, disrupt operations, and affect customer service. Indeed, vulnerability linked to third-party supply chain partners is a critical aspect of cyber risk that many organizations overlook, and third-party breaches have been on the rise. A recent study by AIG reported that over 60 percent of breaches happen through a third party.

Our interviews revealed, however, that most supply chain managers are almost totally unaware of where and how third-party risks may impact them. Managers remain highly company-centric in addressing risks. Furthermore, because organizations don't know how to characterize the threat, they often assign responsibility for cybersecurity to the IT or legal department. But this limited, siloed approach ultimately increases vulnerabilities throughout the supply chain. Senior executives struggle to determine the appropriate level of investment in cybersecurity, often making siloed decisions that do not take into consideration other critical nodes in the supply chain. Additionally, organizations fail to make joint investments on cybersecurity that can pool the resources of the supply chain. The upshot is that supply chain management has yet to develop a systematic approach to cyber risk that sets the stage for success in an increasingly digitalized world.

Benchmark supply chain leaders focus on collaboration to mitigate business risk by working closely with acquisition resources, suppliers, and business partners to bring holistic solutions to reducing risk.

Best Practices In Supply Chain Cyber Security

11 Most Frequently Observed

Although few organizations have cyber supply chain security figured out, our engagement with industry leaders has helped us to put together 14 best practices in this area. The entire best practice follows the case study below. The most frequently observed 11 best practices in Table 1 are discussed below. Many of these best practices build on concepts and capabilities from physical supply chain management, but incorporate key adjustments needed to combat the particular risks involved in cybersecurity.

TABLE 1 CYBER RISK BEST PRACTICES MOST OBSERVED
Catalog
Map processes
Clear Strategy
Critical Systems
Incident Response Plan
Latest Defense Systems
Ongoing Training and Awareness
Use AI and ML Wisely (increases cyber risk)
Unplug
Treat Cybersecurity Like Supply Chain Work
Active Defense

The first step toward cybersecurity is understanding your supply chain and **cataloging your cyber inventory**. Leading edge organizations spend time mapping supply chain nodes and transitions in a way that provides visibility into the people and processes that rely on the information technology systems used in the supply chain as well as existing risk protections (e.g. firewalls). As part of this mapping process, managers catalogue their cyber inventory (hardware and software). Cataloging cyber inventory is a critical step in the **mapping process**, as a risk protection strategy cannot be effective without knowledge of the systems. Overall, mapping the cyber supply chain creates knowledge of the cyber environment and a visual representation of potential "hot spots."

Next, leading organizations create a clear **cyber risk strategy** that explicitly addresses critical choices and directs the work needed to improve cybersecurity. This strategy work includes identifying business critical systems used to manage proprietary information and information vital to short- and long-term business success. More aggressive cyber risk management controls are then built in for these **critical business systems**. A cyber risk strategy should also include a **clear incident response** plan that can be followed in the event of an attack.

Continuous improvement also represents a key element of best practice supply chain cybersecurity. These are lots of ways leading companies incorporate continuous improvement on supply chain cybersecurity. Some of the approaches we've seen include: ongoing systems updates that include the **latest and most effective defense systems** (e.g. firewalls, intrusion detection, and endpoint security); cross-functional collaboration (particularly among engineering, IT, and procurement) to validate incoming equipment and systems for cyber risk; cross-functional collaboration (particularly among logistics, manufacturing, IT, procurement, and other SC disciplines) to validate suppliers, external manufacturing, 3PLs, and other partner cyber systems that interface with business systems; and collaboration with the E2E supply chain to ensure risks and protections are being communicated in a timely and effect manner. All of these ongoing continuous actions help to ensure that a company's risk strategy remains update in a dynamic cyber risk environment.

The people dimension of cybersecurity also needs to be a top priority. The days of annual cyber risk training and knowledge verification are over. **Training and awareness must be ongoing** and should include experiential trainings that test user responses to specific scenarios. As part of addressing the people dimension of cybersecurity, leading organizations have become much more intentional in how they digitize their supply chains. As noted above, supply chain digitalization creates significant new capabilities, but **new tools**, such as artificial intelligence (**AI**) and Machine Learning (**ML**), also **increase cyber risk**. Leading organizations therefore consider which systems really need to be connected and which systems can be **"unplugged"** without sacrificing significant benefits.

Finally, leading edge organizations lean heavily on traditional supply chain management capabilities to ensure the cybersecurity of their supply chains. Benchmark **companies treat cybersecurity capability like improving any supply chain capability.** Thus, these organizations utilize proven supply chain tools and resources to solve cyber risk issues, such as rigorous scorecards, action planning, and leadership reviews; proven lean, total quality, and six sigma problem solving processes; and push continuous supply chain skill and capability development. Most importantly, leading organizations utilize E2E strategic concepts and principles (such as collaboration, integration, and synchronization) to work on cyber risk with their supply chain partners.

The supply chain cyber risk environment is extraordinarily dynamic. So while the techniques outlined above represent best practices, leading edge companies are also on the lookout for new ways to protect their supply chains. For instance, one of the latest approaches to combating cyber risks is actively defending your systems through the use of decoys, misdirection, and other **active defense tools**. Managers should note that active defense tools have ethical and legal implications that go beyond the scope of this white paper and need to be thoroughly researched. Still, we mention active defense as just one of many emerging techniques that supply chain mangers should be aware of as they develop their own robust supply chain cybersecurity plan.

The Four Fundamentals

Our interviews uncovered four fundamentals that organizations need to consider as they move toward implementing the best practices outlined above. Taken together, these fundamentals give supply chain managers a framework for understanding supply chain cyber risks and putting in place organizational structures and strategic investments to face the challenges they present.

Fundamental #1:
Understanding the Nature of Cyber Risks in the Supply Chain

Managers that we talked with stressed that a lack of understanding remains about the nature of cyber risks in the supply chain. They stressed two main areas in this regard:

1. Understanding the types and sources of cyber risk
2. Using a quantitative approach to assessing the potential impact of risks

Types and Sources of Risk

Most managers have an awareness – and perhaps even an unpleasant experience with – cyber risks such as malware, fraud, denial of service, ransomware, and phishing. These represent some of the types of cyber risks that organizations face. More comprehensively, cyber risks can be classified into nine types[viii]:

- Cyber-espionage
- Denial of service (DOS) attacks
- Crime ware
- Web app attacks
- Insider misuse
- Miscellaneous errors
- Physical theft and loss
- Information skimmers
- Point of sale intrusions

Less well understood are the various sources of cyber risks. Here there are no settled classifications. But our conversations with managers did suggest several ways that organizations can start to think about the sources of supply chain cyber risk by asking three simple questions: *Who? How? What?*

Who? As noted earlier, one important way to think about the source of cyber risk is to consider whether the attacker is strategic (i.e. targeting a specific individual or organization for a specific purpose) or non-strategic (i.e. randomly attempting to breach an organization's systems without having a specific target). Strategic and non-strategic attackers can be further categorized in terms of whether they are state-sponsored, state-affiliated, criminal, or general cyber attackers.

Understanding the differences between these types of attackers and evaluating the level of exposure to each is critical to determining financial investments to defend against cyber risks, as discussed later in Fundamental #4.

A significant source of risk comes from individuals,

often within a company's supply chain, that have no malicious intentions at all.

Not all cyber risks come from cyber attackers. A significant source of risk comes from individuals, often within a company's supply chain, that have no malicious intentions at all. For instance, information leaks are usually a result of individuals within the company accidentally sharing sensitive data – not an outside attacker. Such leaks could include sharing internal files, company data, and data on a company's senior executives with others that should not have access to such information for a variety of business or security reasons.

Further, while cloud computing provides new possibilities for companies, it also opens up new risks for information security, user access, regulatory compliance, data location and availability, and disaster recovery. None of these risks are inherently the result of malicious attackers.

How? Another way to categorize the sources of cyber risks is to examine how attackers got in – or how information got out. While most organizations focus on securing their management information systems, they overlook weak links or easy backdoor entry points in their supply chain partners. But supply chain partners (suppliers, distributors, retailers) have the potential to expose a wealth of customer and product information. We found, for example, that cybersecurity is particularly a challenge for manufacturers using emerging technologies, where weaknesses in design systems have yet to be fully identified and production controls have yet to be put in place. One way to think about cyber risks, then, is to develop a holistic view of critical points in the supply chains that potentially could be vulnerable to a breach, whether those points are internal to the organization or at some node in its global supply chain.

Along these same lines, organizations need to consider both the technological and human components of cyber risks. Technological components can include manipulation of data and services, hacking, and viruses. Human components include the processes regularly used by employees that enable the attack. Both the technological and human components play a role in understanding how a cyber attack was perpetrated or an information breach occurred.

What? Finally, organizations can categorize the sources of cyber risk in terms of what is at risk. From a supply chain perspective, we found that four main types of processes are especially subject to cyber risks: processes for managing information about demand, processes for managing physical flow of goods, processes for managing financial flows, and processes for order management. Within these overarching processes are a number of more specific functional sub-processes that rely on systems particularly vulnerable to cyber risks. These include purchasing and supplier management, order management and customer relationship management, inventory monitoring and forecasting, manufacturing control, and management of financial payments. Our conversations suggested that the networks, computers, and devices used to manage these processes across the supply chain were especially vulnerable to cyber risks like password sniffing/cracking software, spoofing attacks, denial of service attacks, and direct attacks like hacking.

Physical assets throughout the supply chain can also be a source of cyber risks.

In addition, physical assets throughout the supply chain can also be a source of cyber risks. For example, attackers may want to breach or manipulate products or parts that include a technology or software component. The use of radio-frequency identification (RFIDs) in global supply chains is particularly problematic in this regard. Unprotected RFIDs can be vulnerable to eavesdropping, unauthorized tracking, insertion of fraudulent tags and readers, denial of service, and other types of tampering.

Global production for both the physical and digital aspects of the cyber supply chain add another dimension of complexity. Many of the physical components of the cyber supply chain are produced in China, Japan, South Korea, and Taiwan. Software development, however, is just as globalized, with many company's outsourcing coding to India, Ukraine, Poland, and the Philippines. Global suppliers for both physical and digital components of the cyber supply chain can be a significant source risk if not properly managed. Categorizing the sources of cyber risks in terms of "Who? How? What?" are useful ways for managers to start thinking about securing their supply chains. But managers also need to keep in mind that as cyber risks continue to evolve, new sources of risk are likely to emerge. Take, for example, the widespread use of e-marketplaces. This new way of doing business brings new risks related to ensuring the legitimacy of the participating members, security of data transmission, maintenance of data, and the availability of accurate and complete information. Document forgery, counterfeiting, corporate identity theft, and the growth of bogus companies were also mentioned as emergent cyber risks in our discussions with supply chain managers. Such nascent threats are difficult to assess and mitigate because of the data needed for trend analysis is lacking. Nevertheless, these cyber risks can have serious implications for physical assets, like cargo in transit, reverse flows, and human resources.

Although managers' first reaction to a quantitative approach might be to emphasize the difficulty in quantifying cyber risks,

we have found that the process is typically simpler – and far more accurate – than what most organizations currently use.

Impact of the Risk

Effective risk management relies on assessing the potential impact of risks. Risk assessment is especially important for cyber risks, as the impact may have a domino effect on many levels. Most managers use a qualitative approach to risk assessment, often using a color-coded scale or dimensions of high and low. But a qualitative approach is highly problematic when assessing the impact of unique and complex risks. Rather, a quantitative approach is necessary to rigorously assess cyber risks. Although managers' first reaction to a quantitative approach might be to emphasize the difficulty in quantifying cyber risks, we have found that the process is typically simpler – and far more accurate – than what most organizations currently use.

The concern with using a purely qualitative approach to examining cyber risks in supply chains is that it adds another layer of ambiguity to the process. Risk assessment should provide clarity on what the risks are and their potential implications. But because cyber risks are not well understood to begin with, labeling them high/medium/low or using a color-coded scheme is often extremely misleading. The term "high risk" can mean many different things to people within an organization and even more so across organizations. A simple exercise used across all categories of risk management, but especially appropriate for cyber risk assessment, is to ask a group of people to write down a percentage between 0-100 of the likelihood of a "high risk" occurring. We've found people's expectations ranged anywhere from 40 percent to 99 percent. Imagine now the confusion this term introduces in a global supply chain with hundreds and thousands of people from different disciplines and backgrounds. The same thing applies to the concept of potential impact. What does "high impact" mean? Does that mean that the expected losses are $10,000, $10 million, or $10 billion? You get the picture.

Although there are challenges with assigning numbers to the expected probability and losses associated with an event, this process in itself brings clarity on what cyber risks mean to the supply chain. And there are ways to make this type of quantitative approach manageable. For instance, probabilities and expected losses do not necessarily need to be assigned specific numbers, but can be assigned a range. Even a wide range for probabilities and expected losses will yield a more accurate and consistent process for examining and quantifying cyber risks.

Once probabilities and expected losses are assigned to each risk, the rest is simple. Statistical simulation techniques, such as Monte Carlo simulation[xii] available in Microsoft Excel, can be used to quickly provide a range of expected losses for the year. The entire process can be done with the involvement of different groups from the organization in less than half a day. The output of the simulation can then be compared to a company's risk tolerance in a given situation (Figure 1). This process should never be treated as a static result. Rather, it should be a continuous monitoring system based on the dynamic nature of cyber risks.

Figure 1: Comparing Simulation Results to Organizational Risk Tolerance

Risk Management of Critical Business Systems

In the cyber risk best practice section above, the importance of understanding the critical business systems is arguably the most important practice. The critical business systems include proprietary information/devices/equipment and information critical to the enterprises success. In our research, we obsevrved that the benchmark companies treat the risk management of these system differently

Best Practice: Critical System Risk Management

Benchmark firms use aggressive cyber risk management activities for the critical supply chain system - those systems with proprietary data or data vital to short- and long-term business success. Such activities include:

1. Unplug these systems from the internet.
    - Over 60 percent of cybersecurity issues occur in third parties working in supply chains. How strong are the cybersecurity capabilities of 3PL and external manufacturing?
2. Avoid IoT, cloud computing (processing and storage), AI, and ML.
3. Choose to utilize a small group of highly qualified people to manage the system (over more automated digital solutions).
4. Mandate software upgrades as soon as an update is available (versus systems that allow users to decide a convenient time to upgrade software).
5. Hold weekly, experiential cyber training and awareness.
6. Add multiple-step password verification.
7. Deploy aggressive defense systems and management, such as
    a. Trip wire detection
    b. Air gaps buffers
8. Mandate monthly cyber supply chain map reviews and problem solving

Fundamental #1 can be summed up as follows: to build cybersecurity in the supply chain, you first need to wrap your head around what the risks are and what their potential impact is. In our discussions, we found that the key is understanding:

- Sources of cyber risk and assessing the risks using a quantitative approach.
- More aggressive risk management for critical business systems

Fundamental #2:
Developing a Cyber Risk Management Strategy and Culture Within Your Supply Chain

In order to address supply chain cyber risks, there needs to be a clear and explicit strategy in place. Organizations may elect to pursue different strategies depending on the nature of their industry, product type, potential risk exposure, and risk tolerance. Strategies may take the form of trying to strengthen the security perimeter in the hopes of preventing or minimizing any attacks. Other strategies may be designed on the concept of resiliency. A resilience strategy focuses on how to respond and bounce back from a breach in supply chain cybersecurity. Some organizations operate under the premise that at any point in time, there is one machine or device in the supply chain that is breached, and all decisions should be planned according to this assumption. Organizations may also use a combination of preventive and resilience strategies in a hybrid form that is a better fit for their environment and needs. Elements for structuring a cyber risk mitigation strategy may also be from an existing framework.

Supply chain managers do not need to recreate the wheel

as they seek to develop a cybersecurity strategy.

Cyber Risk Management Frameworks

Numerous strategy frameworks exist for information and technology management. These include ISO 27001 and ISO 27002, ITIL (formerly Information Technology Infrastructure Library), and COBIT (Control Objectives for Information and Related Technology). The National Institute of Standards and Technology (NIST) has produced perhaps the most robust framework specifically related to cybersecurity. Table 2 lists some cyber risk management frameworks.

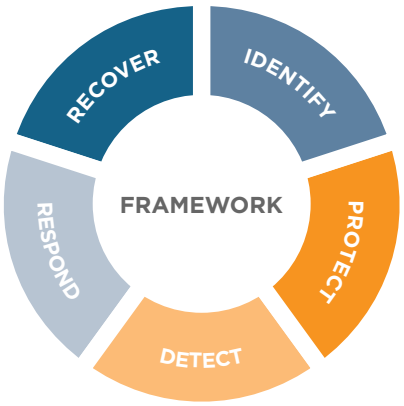
TABLE 2 - EXAMPLE CYBER RISK MANAGEMENT FRAMEWORKS		
ASD	CCPA	CIS
COBIT	EU GDPR	HIPAA
HISO	ISO 27k	ITIL
NIST	NZISM	PCI DSS

Copious documentation for these frameworks exists online, and several of the sponsor organizations offer certifications. We will look a bit more closely at the NIST Framework below, but the point here is not to discuss all of these frameworks in detail. The point, instead, is that supply chain managers do not need to recreate the wheel as they seek to develop a cybersecurity strategy. Any of these frameworks could serve as the basis for developing a holistic cybersecurity strategy.

The NIST Framework[ix] (portrayed in Figure 2) is one of the most commonly used for cyber risk management. NIST is a voluntary framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk. The framework was created to help promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. The central value of the NIST Framework is that it provides a common language, which anyone can understand, for talking about cyber risk. It therefore allows a wide range of stakeholders to adapt the framework to their particular technologies, lifecycle phases, sectors, and uses, while ensuring everyone is on the same page. The framework also describes implementation tiers that can be used as benchmarks to assess an organization on both prevention and reaction. In this way, the NIST Framework (Figure 2) drives organizations toward a more evolutionary approach – one that is risk-based and focused on achieving desired outcomes.

The NIST framework provides significant detail regarding implementation of five foundational functions of cybersecurity risk management. *Identify* focuses on the need to establish an organizational understanding of the top cybersecurity risks to systems, assets, data, and capabilities. *Protect* involves developing and implementing appropriate safeguards to ensure the safeguarding of critical infrastructure services. *Detect* provides insights to develop the ability to identify the occurrence of a cybersecurity event. *Respond* relates to steps required to take action regarding a detected cybersecurity incident. Finally, *Recover* involves planning for resilience and restoration of capabilities or services that were impaired due to a cybersecurity security event.

Figure 2:
NIST Framework



As we noted, the NIST Framework is just one of several well-developed models that companies can build on for their cybersecurity strategy. In other words, the resources are out there already. Supply chain managers can adopt or adapt these frameworks as needed. Most importantly, though, supply chain managers need to develop a culture that supports whatever risk mitigation strategy they choose to pursue.

An organization's culture is influenced

by the norms of behavior and attitudes that are present in a company.

Culture of Supply Chain Cyber Risk Management

Easily the most difficult—and certainly an important—way to achieve a low risk cyber supply system is through influencing the people systems[xi] (organizational culture).

An organization's culture is influenced by the norms of behavior and attitudes that are present in a company. How people think, how they interact with others, what they find important, how hard they work, how they dress—all of these factors and countless others define an organization's culture.[xi] One of the paramount challenges in cybersecurity capability is that this culture must be developed across the end-to-end supply system, therefore crossing company boundaries.

The norms and behaviors are largely created by the people systems. Rewards, rituals, promotions, compensation, communication, problem solving, celebration, and role modeling are a few of the key systems/activities that strongly influence norms and behavior.

Some organizational cultures support strong cybersecurity capability and some resist it. Resistant cultures are characterized by each functional group or supply partner having its own unique culture, with people being distrustful, or even disdainful, of other functional groups' cultures. Cultures that promote cybersecurity capability encourage the pursuit of total value through seamless, collaborative, end-to-end integrated systems, regardless of the functional area or company in which personnel work.

Most benchmark companies creating end-to-end cybersecurity capability establish common cyber principles, values, ands standards. Then ensure all of the business functions and corporate systems support full collaboration to achieve the business goals.

Characteristics of the benchmark cultures include:

- End-to-end supply system has common standards, values, and principles
- Learning culture exists across boundaries
- Rewarding attention to detail and a deep understanding of the risk management best practices is celebrated across all systems
- Continuous improvement of cultural systems to cyber capability improvement
- Overlapping functional and company rewards systems (including executive leadership compensation systems)
- Celebrating total value improvement (jointly with supply partners)
- Cross discipline, company, and functional collaboration

The combination of an effective strategy and a cultural change within and across organizations presents the real first step in a meaningful approach to combating supply chain cyber risks.

The combination of an effective strategy and a cultural change within and across organizations presents the real first step in a meaningful approach to combating supply chain cyber risks. The focal organization as well as its key suppliers and customers should follow a consistent supply chain cyber risk management strategy, which adheres to a framework (existing or internal). This can be achieved only when there is a true cultural change and a different mindset in dealing and managing such risks.

Benchmark supply chain leaders focus on total involvement in mitigating cyber risks. Total involvement entails two key elements:

1. The recognition that all people and technologies operating in a cyber environment represent a potential source of cyber risk
2. A culture built around the idea that cybersecurity is a complex problem that requires the brainpower and energy of 100 percent of the organization to achieve

Fundamental #3:
Integrating with Key Partners to Manage Cyber Risks in the Supply Chain

Supply chain integration has been addressed in a separate white paper and represents one component of the larger GSCI End-to-End Supply Chain Improvement Model developed at the University of Tennessee. We define supply chain integration as the process of connecting decisions and actions across an end-to-end supply chain (supplier's supplier to consumption) to drive total value for all stakeholders.

Supply chain integration requires aligning strategies, effectively managing operations, and maintaining reciprocal flows of information among stakeholders to consistently optimize results for the entire supply chain. This means having a united and cohesive supply chain team within your company's four walls, which includes not only the typical supply chain functions, but also representation from other major functional areas such as IT, finance, and marketing. It also means working with supply chain partners to achieve well-defined goals that are based on a common understanding of the value that is being created for stakeholders and consumers.

Many companies still work on the assumption that they can operate within their four walls

Many companies, however, still work on the assumption that they can operate within their four walls, taking orders as they come from customers and relying on suppliers to ensure necessary material and service flows. But research has shown, and industry experience has vividly illustrated, that when companies narrowly focus on just their slice of the process—without considering the effects of their decisions on other parts of the supply chain—total supply chain performance suffers.

Nowhere is this truer than in combating cyber risks. Supply chain integration needs to be a fundamental aspect of overall cybersecurity. In the context of cybersecurity, integration focuses on three levels: functional, organizational, and end-to-end supply chain. In a sense, these levels represent an evolution in thinking about and responding to cyber risks in the supply chain. As companies' thinking about cyber risks matures, they should be building out from a functional focus, to an organizational focus, and then finally to an end-to-end supply chain focus (Figure 3) – while retaining best practices and lessons learned at each stage of development.

Figure 3: Organization Focus

Functional Focus

This is where most organizations focus their efforts in managing cyber risks. Typically, a specific functional unit, often the information and technology (IT) department, is assigned responsibility for managing the cybersecurity problem. This functional focus is usually reinforced by norms within the organizational culture that emphasize channeling all IT-related concerns through the IT department. Other organizational stereotypes, such as that IT employees are the best suited to deal with this issue since it is a technology-related risk, also come into play. In some organizations, the legal department handles cyber risks. The view typically expressed in these organizations is that cybersecurity represents a compliance issue, and therefore the general counsel should deal with it. More than anything, these and similarly functional focus approaches reflect a limited ability on the part of an organization to wholly comprehend the full range of cyber risks, how these risks are embedded in broader supply chain relationships, and what the potential impact of these risks are on operations, financials, brand perception, and other metrics.

...this is not an IT or legal issue,

but rather a serious business risk that needs to be tackled by multiple camps within and across organizations.

Starting with a functional focus can provide organizations with a foundation of knowledge and experience that can then be transferred to other parts of the supply chain. However, although a successful cybersecurity strategy can have a functional lead, it is nearly impossible to effectively combat cyber risks with merely a functional focus in place. The transition in maturity of integration starts with a shift in mindset throughout the organization (and supply chain) that this is not an IT or legal issue, but rather a serious business risk that needs to be tackled by multiple camps within and across organizations.

Organizational Focus

An expanded view of cyber risks includes multiple functions within the organizations becoming involved in formulating the strategy and dealing with the risk. Managers in such organizations realize that cyber risks represent an organization-wide concern that needs to be addressed with the participation of several units, not just the IT department. This more integrated approach could include creating a Chief Information Security Officer (CISO), who would be charged with coordinating cybersecurity with the CIO, COO, and other executives involved in supply chain management. It would also likely involve creating a systems security plan (SSP). An SSP details current meausres for securing a company's information systems and provides a critical starting point for improving those cybersecurity processes.

While an improvement on the functional focus approach to cybersecurity, the organizational focus approach still lacks the involvement of other members of the supply chain. This leaves companies vulnerable, because the weakest link in their cybersecurity strategy may well be a third-party provider. As we discuss below, investments decision related to cybersecurity are typically suboptimal without an end-to-end supply chain approach.

> Benchmark supply chain leaders focus on end-to-end integration to strengthen the weakest link in their supply chain and mitigate cyber risks.

End-to-End Supply Chain Focus

Having a supply chain-wide view when addressing the scope of supply chain cyber risks is necessary to have an effective strategy.

Having a supply chain-wide view when addressing the scope of supply chain cyber risks is necessary to have an effective strategy. As with other E2E supply chain initiatives, E2E integration concerning cybersecurity rests on three core components: supply chain collaboration, end-to-end process management, and reciprocal flows of high-quality information to enable decision making.

- As discussed in another GSCI white paper in the Innovations in Supply Chain series, supply chain collaboration is the process of working with strategic partners to identify, define, and pursue specific business opportunities that have the potential to increase overall supply chain value. In the context of supply chain cyber risk management, collaboration must start with a common understanding of (1) the types and sources of cyber risk impacting the supply chain, (2) a quantitative assessment of probabilities and expected losses associated with relevant risks, and (3) identification of the greatest opportunities and challenges that need to be addressed. Achieving this common understanding requires detailed mapping of the supply chain, from suppliers' suppliers to end users.

Making informed cybersecurity decisions requires data analytics *that provide real-time information for leadership and management.*

- End-to-end process management focuses on linking decision making across the supply chain into a single, seamless process that supports cybersecurity. As with everything else in supply chain management, decisions regarding E2E process management must be made in the context of evaluating trade-offs. Perhaps most important for understanding these trade-offs is learning about the kind of threats the supply chain faces and how investments should be made. Fundamental #4 discusses these decisions in detail.
- Data and information are perhaps the most important tools supply chain managers have to combat cyber risks. Making informed cybersecurity decisions requires data analytics that provide real-time information for leadership and management. Data analytics can create more proactive and ultimately predictive decision making throughout the supply chain. Key here is that data on current and emerging cyber threats be relevant to the decisions being made and organized to focus decision makers' attention on situations that require action, while at the same time being adaptable for different users.

Best Practice Example:

Leading-edge companies are using a number of end-to-end strategies to prevent and mitigate cyber attacks. For instance, companies we talked to stressed the importance of segmenting data and then working with supply chain partners to create protocols that clearly define who has access to what. Segmenting data and controlling access allows companies to quickly quarantine systems in case of a breach and to have a better understanding of what has been compromised. These companies are also working with supply chain partners to gather incident data, so advanced data analytics can be used to catch vulnerabilities before they turn into a costly security failure.

Integration can start internally across the functional areas within a company or externally with upstream and downstream partners. Either way, companies need to focus on the three central elements of supply chain integration: collaboration, end-to-end process management, and reciprocal flows of high-quality information. Each of these elements supports the overall objective of achieving the cybersecurity needed to enable the supply chain to create value for its stakeholders.

Approaches that focus on a specific function or an organization are guaranteed to have blind spots in their strategy. Few organizations manage their cyber risks in an end-to-end, systematic approach. Some organizations will require some of their suppliers to be certified, but a full analysis of the risks and the weakest links in the supply chain is still rare in practice. This means that leading organizations have a major opportunity to adopt risk strategies that can differentiate them in them in today's increasingly digital marketplace.

Benchmark supply chain leaders focus on end-to-end supply chain integration to mitigate cyber risks in the internal and external operating environment.

Senior executives

are constantly trying to determine the appropriate levels of investments in cybersecurity

Fundamental #4:
Deciding Where to Invest Resources to Protect Your Supply Chain

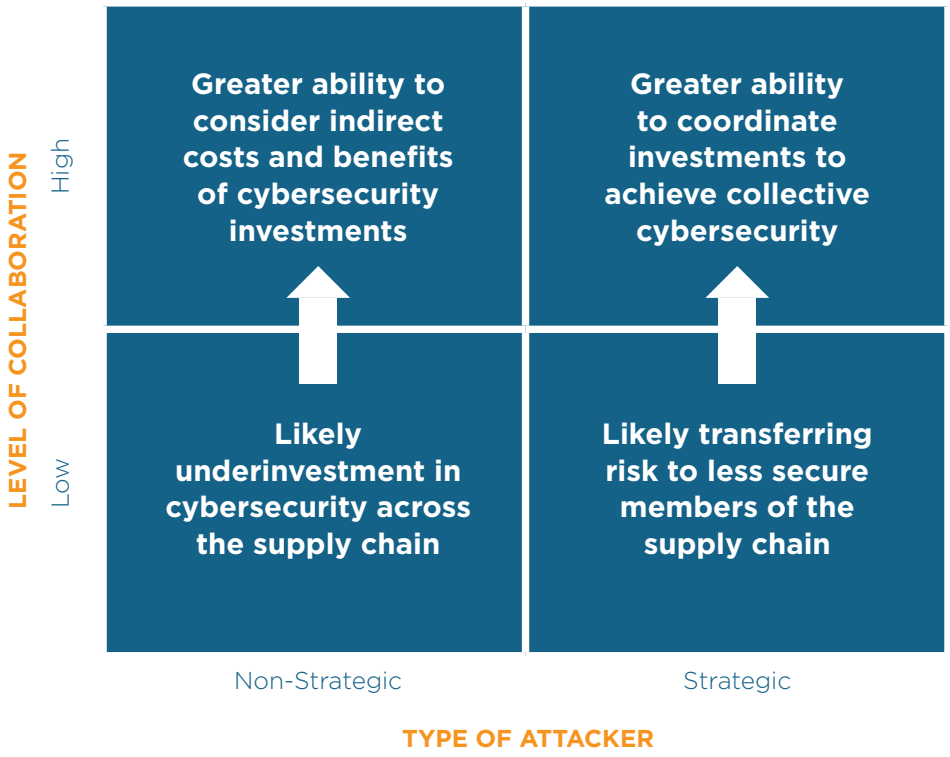
Senior executives are constantly trying to determine the appropriate levels of investments in cybersecurity, but most investment decisions are made in silos without taking other critical organizations in the supply chain into consideration. For example, a large retailer might invest substantial sums of money to keep customer data protected, as the negative publicity and loss of trust associated with a breach would carry an enormous cost. However, a supplier with whom the retailer shares customer data might be less motivated to do so, since the cost of a breach to the supplier is relatively small. In general, cyber attacks on a firm include both direct costs to that firm as well as indirect costs to other firms in its supply chain. Improving the operational and financial performance of companies within a supply chain is only achieved when there is some level of collaboration in place, and cybersecurity investment decisions are no different. Without explicit collaboration, it is unlikely that these firms will act in a way that is optimal for the overall supply chain.

In our discussions, we analyzed the differences between collaborative and non-collaborative cybersecurity investments as well as the differences resulting from a strategic and a non-strategic attacker. We found that lack of collaboration leads to underinvestment with a non-strategic attacker, although this is somewhat counterbalanced by an attacker being strategic. Lack of collaboration may lead to either underinvestment or overinvestment with a strategic attacker, depending on how large the indirect damages from attacks are relative to the direct damages; overinvestment is more likely if indirect damages are relatively minor.

One way of examining the optimal levels of investments to manage cyber risks is using a game theory approach called an *attacker-defender model*, which is commonly used in counterterrorism. In this approach, each of the firms in the supply chain is a defender and must choose how much to invest in cybersecurity. The attacker observes these investment levels, and then has some probability of targeting each firm in the supply chain. The attacker is not a specific person or group; (s)he is meant to be representative of a population of potential attackers. The attacker-defender model can be depicted in a 2x2 matrix as follows: (1) whether or not the attacker is strategic, (i.e. the attacker attacks specific or more appealing targets more often,) and (2) whether the defenders' cybersecurity investment decisions are collaborative or made independently. The 2x2 matrix depicts some of the different scenarios that an organization can examine to determine optimal levels of investment. Different variables can be used to frame the analysis based on different sectors or threats.

Attacker-defender models (simple example in Figure 4) have been applied widely in the context of terrorism, where the defender is a nation or other decision-making entity determining an optimal investment of resources.

Figure 4: Example Attacker-Defender Model



Running a simulation based on this design leads to some interesting findings:

1. First and foremost, if attackers are not strategic (i.e. they simply attack firms randomly) and firms (defenders) do not collaborate, they will systematically underinvest in cybersecurity. When firms do not collaborate, they tend to consider only the direct costs and benefits of their investments. However, they tend to ignore significant indirect costs and benfits that come from their supply chain. Moreover, they tend not to consider the impact (positive and negative) their investments have on supply chain partners. In other words, a lack of collaboration creates blind spots with regard to the true costs and benefits of cybersecurity investments, and therefore skews decsions on where and how to invest to manage cyber risks.
2. The more interdependent noncollaborative firms are, the more they tend to misallocate cybersecurity investments aimed at protecting against nonstrategic attacks. In other words, noncollaborative firms tend to misallocate investments the most exactly when a nonstrategic attack has the largest potential to affect the supply chain as a whole. And it gets worse: over time the lack of investment among noncollaborative firms tends to grow, further increasing vulnerabilities to nonstrategic attackers. Under these conditions, it is critical for firms to adopt an end-to-end supply chain collaboration approach, as dicussed in a previous GSCI white papers[x], to map out the mutual benefits of a collaborative cybersecurity strategy.
3. If an attacker is strategic (that is, focused on penetrating your particular network), noncollaborative firms do tend to increase cybersecurity investments. But while increasing investment in response to a strategic attacker may reduce risks for the focal firm, it actually increases risks for

A lack of collaboration creates blind spots

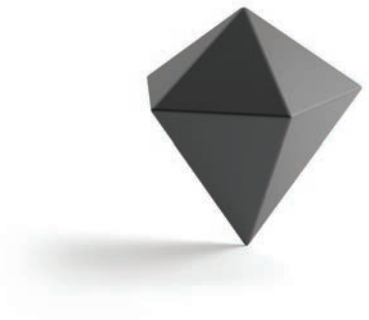
with regard to the true costs and benefits of cybersecurity investments, and therefore skews decsions on where and how to invest to manage cyber risks.

the supply chain as a whole, by essentially transferring the risk from more secure to less secure members of the supply chain. In other words, when a firm ignores its supply chain partners and focuses solely on making itself more secure, it tends to shift a strategic attacker's attention to less secure members of the supply chain. This shift means that vulnerable suppliers or other third-party providers will now be more aggressively targeted than before. The net result is an overall increase in cyber risks to the supply chain that undermine individual investments made to protect against strategic attackers.

4. The risk transfer problem that occurs in response to strategic attackers is worse when companies in the supply chain are less interdependent. In other words, in loosely connected supply chains where companies interact across a wide network of suppliers and customers, stronger more capable firms will invest to protect themselves, which has the effect of transferring risks to weaker more vulnerable firms in the supply chain. This risk transfer problem can only be addressed through collaborative investment decisions. For example, under these conditions, it may make sense for dominant supply chain players to invest in consortiums or other types of collective associations that can help to improve the cybersecurity programs of vulnerable third parties.

...firms develop collaborative mechanisms for coordinating and modeling their cybersecurity investments...

As with most collaboration efforts, supply chain managers' ability to define and create value for all supply chain partners is the biggest challenge. Managers must use an end-to-end process to determine how much supply chain value is put at risk by various kinds of strategic and nonstrategic cyber threats. Collaboration on cybersecurity investments can then be used to systematically limit the misallocation of resources and any potentially negative unintended consequences. Although difficult, it is absolutely critical that firms develop collaborative mechanisms for coordinating and modeling their cybersecurity investments with other supply chain firms if they hope to manage the cyber threats they face.



Case Study

In writing this white paper, we talked to numerous companies that have been developing leading-edge cyber risk mitigation strategies in their supply chains. Here we will discuss in depth some standout strategies we found.

These strategies come from several large providers of primary information technology services working in the aerospace, defense, and security industries. Because of their involvement in sensitive, national security-related cyber services, these primary service providers have years of experience in developing a robust cybersecurity posture.

That doesn't mean cyber breaches never occur. These primary service providers rely on a broad base of smaller organizations in their supply chain, many of which have far less ability – or incentive – to manage cyber risks. One story that was shared started with a major customer reporting a problem to a primary service provider. The problem was occurring on a server that had been running on the customer's network for a number of years. As the primary service provider investigated the problem, they realized the server was running an unauthorized memory system. It turned out that a value added reseller (VAR) had purchased the server from an OEM and then inserted the unauthorized memory system to reduce costs. The change was never reported and ultimately ended up being installed in the customer's network. Nightmare scenarios like this drive many of the cybersecurity strategies we saw in this industry.

First and foremost, industry leaders we talked to stressed the need for a shift in mindset from compliance to maturity. Instead of beating up suppliers for non-compliance, industry leaders have focused on developing standards and maturity models that are far more developmental. Doing so offers suppliers a path toward maturity that encourages learning and continuous improvement in cybersecurity.

Along these same lines, industry leaders focus on education through publishing best practices and experiences, socializing best practices through high-profile users, cases, blogs, and videos, and even offering services in implementing best practices. They also work closely with government and standards-setting organizations, such as NIST and ISO, as well as credible non-regulatory organizations, such as the Center for Internet Security and Cloud Security Alliance. All of these

efforts help to create a culture of cybersecurity in the industry and make it much easier to talk with supply chain partners about risk mitigation strategies.

In managing the supply base, the focus has been on supplier rationalization, traceability, and certification. One company we talked to went from 155 VARs in their supply chain down to 24 VARs. Beyond the normal benefits of better spend management and closer relationships, rationalization helped the company verify suppliers' cybersecurity programs. The company now works with 12 primary VARs and 12 developmental VARs to ensure cyber risk management through traceability audits. With 155 suppliers, it would have taken a small army to complete traceability audits. Now, once a quarter, the company randomly pulls purchase orders and requires their VARs to provide objective evidence on the chain of custody for products back to the OEM.

Internally, these industry leaders also have robust security plans for every project. Security plans often involve a cross-functional team that includes representatives from the IT, legal, and purchasing departments. Teams work collaboratively to ensure third parties are not introducing risk through hardware or software. Because critical suppliers might still not have the full range of desired cybersecurity capabilities, alternative solutions are often needed. One service provider, for instance, will sometimes bring subcontractors onto their in-house network. By running all devices, software, and connections through the internal network, they ensure a high degree of cyber risk management.

Not surprisingly, industry leaders we spoke to emphasized that sound supply chain and quality management practices provide an important foundation for developing and improving cybersecurity processes. Inventory management was one of the most important supply chain concepts that came up in our discussions. In cyberspace, inventory means everything from hardware to software to the code that runs on personal devices and servers. The complexities in managing this inventory are immense, as cyber inventory is rapidly evolving and dispersed across numerous physical and non-physical locations.

Ensuring that users are using the latest hardware and software –

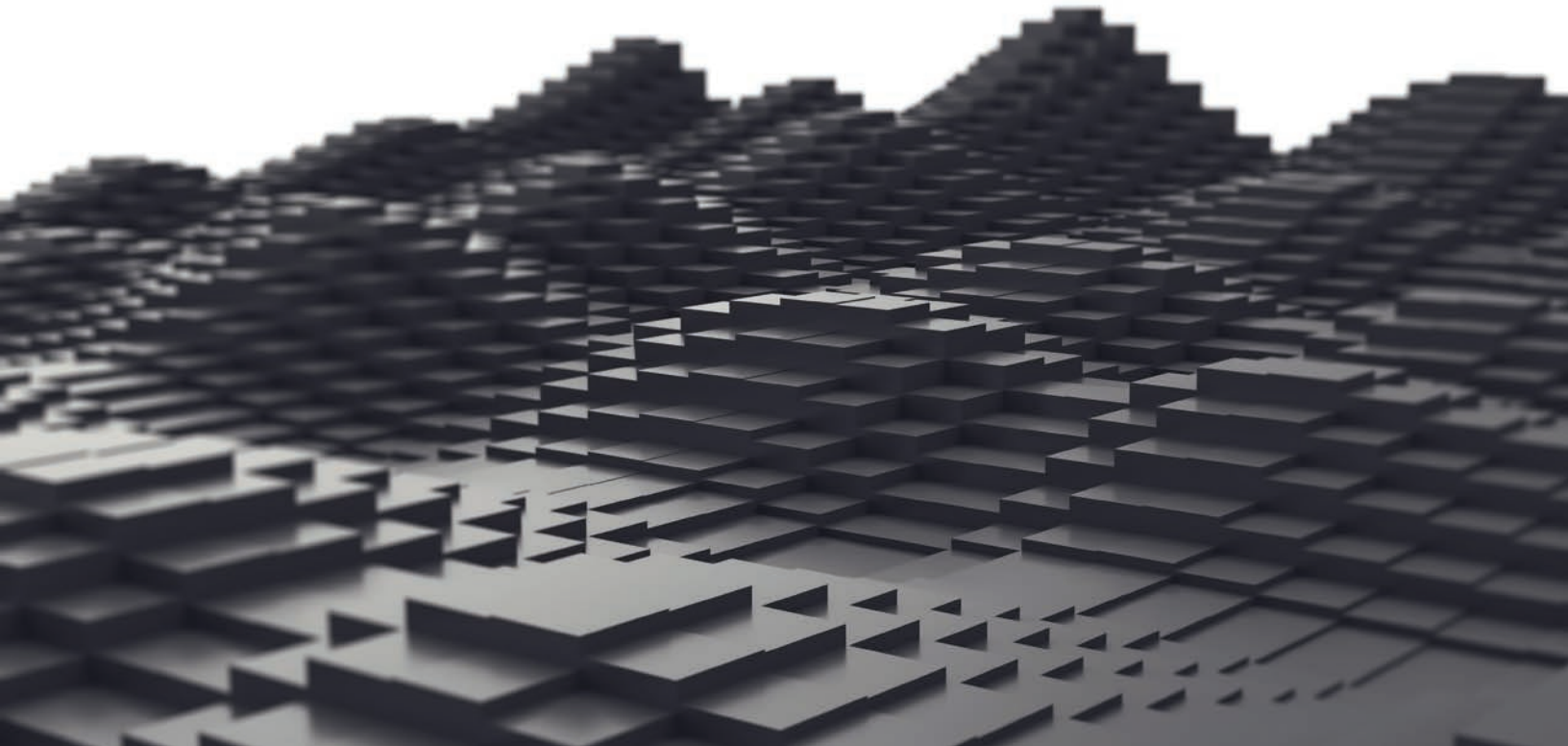
and not straying outside the approved supply chain – is a monumental task.

Ensuring that users are using the latest hardware and software – and not straying outside the approved supply chain – is a monumental task. Leading-edge companies rely on their supply chain to notify them when security issues arise and work collaboratively with these partners to create patches. Internally, they develop tracking systems that help them maintain a database of cyber inventory. Indeed, the companies we talked to suggested that developing systems that maintain accurate records on inventories should remain a major focus in cybersecurity.

Here, too, visibility is key. IT tools, such as Microsoft System Center Configuration Manager, can be used to provide visibility and push software patches. But these systems were not strictly developed for cybersecurity. More recently, there has been a shift toward driving visibility, using tools that are designed specifically for cybersecurity. These tools can enable both asset management, by maintaining a robust database of technology assets, as well as security management, for instance by enabling queries on specific malicious software or vulnerable hardware. Even with these tools, close monitoring is needed, particularly of hardware and software that is run on a corporate system but may not be directly provided through the business.

These companies couple robust inventory management strategies with a zero-trust approach, which simply assumes that users are going to introduce cyber risks into their network and that, therefore, no user should be allowed access to sensitive information without authentication. More generally, the companies we talked to stressed the need to see inventory as owned by a group of stakeholders that have a joint stake in making sure cyber assets are up to date and in compliance with security standards.

Overall, our discussions with leading edge companies suggest supply chain management is intimately linked to cybersecurity efforts. Collaborative capabilities and the experience of working on integration and platform management in the physical supply chain place supply chain professionals in a unique position to foster enhanced cybersecurity in their organizations.



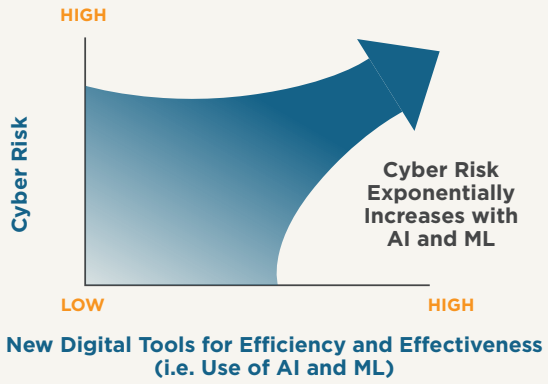
Cyber Risk Best Practices

Based upon the research conducted for this white paper and the other discussions conducted with subject matter experts, the following represent a comprehensive set of 14 best practices to cyber risk management.

- Catalog
  - All of the end-to-end systems (hardware and software systems that could create cyber risk) need to be identified and cataloged. A risk prediction system cannot be effective without knowledge of the systems.
- Map
  - The supply chain nodes and transitions maps (hopefully already completed for other E2E SC strategy work) should be modified to document systems (from "Catalog," above), cyber risk, people interaction and existing risk protection (i.e. firewalls). The mapping process will create knowledge of the process and a visual representation of the "hot spots."
- Strategy
  - A clear cyber risk strategy should be developed to overtly understand the important choices and direct the work.
- Critical Systems
  - Identify all business critical systems. These systems hold proprietary information and information vital to short- and long-term business success. Use more aggressive cyber risk management for critical business systems (see critical system best practices above).
- Response
  - A clear incident response plan should be created (not in the heat of a major issue) and followed in the event of an attack.
- Treat Cyber Like Supply Chain Work
  - Utilize proven supply chain tools and resources to solve cyber risk issues
  - Rigorous scorecards, action planning, and leadership reviews
  - Utilize proven lean, TPM, and six sigma problem solving processes
  - Continuous skill and capability development
- E2E (end-to-end) Integrated
  - Utilize the E2E strategic concepts and principles (collaboration, integration, synchronization) to work supply chain cyber risk holistically.
- Latest Defense Systems
  - Ongoing system to implement the very latest and effective defense systems (i.e. firewalls, intrusion detection, endpoint security)
- Validation
  - Engineering, IT, and procurement partnership to validate incoming equipment and systems for cyber risk protection. This must include the end-to-end supply chain, as the majority of risk is "outside of our walls."
  - Logistics, manufacturing, IT, procurement, and other supply chain disciplines partner to validate suppliers, external manufacturing, 3PLs, and other partner cyber systems that interface with business systems.

- Unplug
  - Systems connected to the internet cannot be cyber-risk free. Unplug critical systems that can be efficiently managed without the internet.
  - Benchmark companies in highly technical, nuclear, information system, and pharmacuetical industries have utilized the "unplug" best practice for a number of years on business critical systems. The focus is on clearly defining the few, critical business systems. Captive systems with dedicated experts to manage the information, control, and equipment (avoid plugging into internet or public systems) are utilized to reduce cyber risk.
  - As cybersecurity risk grows the "unplug" best practice is expanding to less technical industry groups.
- Use AI and ML Wisely
  - The digitalization of the supply chain is creating significant new capabilities important to business success. Conversely, these new tools (such as artificial intelligence [AI] and Machine Learning [ML]) exponentially increase cyber risk.
  - Supply chain tension is created as digital tool utilization is rapidly increasing the efficiency of the supply chain. These digital tools such as AI and ML rapidly find and analyze huge amounts of data (frequently from internet or public systems) to provide leaders with dramatically higher quality information for decision making. Simultaneously, the supply chain is exposed to dramatically higher levels of cyber risk.

Figure 5: Digital Tool Risk



- Ongoing Training and Awareness
  - The days of annual cyber risk training and knowledge verification are over. Training and awareness must be a part of the ongoing system (weekly, experiential).
- Acquisition Integration
  - All acquisition systems must be validated before system integration. This can be a massive task and should be included overtly in the acquisition economics and intergration plan (resources and timeline).
- Active Defense
  - One of the latest tools to combat cyber risk is actively defending your systems (note: this is NOT hacking back). GSCI has included active defense on this best practice list. It has ethical and legal implications and is beyond the scope of this paper. Before you choose to use active defense, the issues and challenges should be thoroughly researched.

Conclusion

Digitalization is allowing supply chains to change in ways that were unimaginable a generation ago.

Digitalization is allowing supply chains to change in ways that were unimaginable a generation ago. At the same time, however, a growing dependence on digital technologies – while in many ways necessary and beneficial – also exposes supply chains to cyber risks that can have a major impact on business performance. As we've stressed throughout this paper, perhaps the most important feature of these new cyber risks is that they can impact a business through the security weaknesses of partner organizations. To build a robust cybersecurity posture in today's complex supply chains, internal and external stakeholders need to work together. Managers need to activate **100 percent total involvement** in understanding the nature of the risk based on a quantitative approach to assessing the probabilities and expected losses from risks. They also need to develop strategies based on established best practices and cultures within their organizations that support cybersecurity. As part of their strategy, organizations need to **integrate** with key partners across the **end-to-end** supply chain to manage cyber risks in the supply chain. And finally, they need to **collaborate** with partners on deciding where (and how much) to invest to protect the supply chain. To guide managers in their efforts, we provide in the appendix a brief checklist for assessing cyber risk management in the supply chain. Cyber risk in the supply chain is a complex and evolving topic – and no organization has it completely figured out. But supply chain leaders must begin to incorporate new cybersecurity strategies into their supply chain management practices or risk facing the fallout.

Appendix

Checklist – The Seven Steps to Supply Chain Cybersecurity

1. Identify a supply chain cyber risk management strategy.
2. Identify (NIST, COBIT, etc.) or develop a framework to be used.
3. Communicate the importance of a cultural change in dealing with such risks (i.e. this is not business as usual), and implement it.
4. Integrate strategies, tactics, etc. within and across key supply chain partners (follow the integration maturity model).
5. Understand the nature, type, and sources of risks that are specific to the organization and industry.
6. Model investments based on the integration maturity model and different types of potential attackers to allocate investments throughout the supply chain.
7. Continuously monitor changes in the environment or threats to make any necessary revisions.

End Notes

[i] Scott, S.; Stank, T. Hazen, B. *A SAVVY Guide to the Digital Supply Chain*. A Global Supply Chain Institute White Paper, 2018.

[ii] Valinsky, J. "Marriott reveals data breach of 500 million Starwood guests"; CNN Business November 30, 2018; (Accessed on date?: https://www.cnn.com/2018/11/30/tech/Marriott-hotels-hacked/index.html).

[iii] Mayer, M.; de Scalzi, N.; Martino, G; Chiarugi, I.; *International Politics in the Digital Age: Power Diffusion or Power Concentration?* Adapted from a paper presented by the authors.

[iv] Congressional Research Service; *Defense Primer: Cyberspace Operations;* Version 4, updated January 2020.

[v] Cebula, J.; Young, L.; *A Taxonomy of Operational Cybersecurity Risks;* Technical Note CMU/SEI-2010-TN-028; Software Engineering Institute; December 2010.

[vi] Biener, C., Eling, M.; Wirfs, J.H.; "Insurability of cyber risk: An empirical analysis." The Geneva Papers on Risk and Insurance-Issues and Practice 40.1, 2015. 131-158.

[vii] McAfee Center for Strategic and International Studies; "Net Losses: Estimating the Global Cost of Cyber-Crime," 2014.

[viii] 2019 Verizon Data Breach Investigations Report.

[ix] NIST Cybersecurity Framework, updated 2020. (Accessed on date?: https://www.nist.gov/cyberframework).

[x] Burnette, M; Dittmann, P ; *End-to-end Supply Chain Collaboration Best Practices.* A Global Supply Chain Institute White Paper 2017

[xi] Burnette, M; Policastro, M; Munyon, T ; *High Performance Organization (HPO) Best Practices.* A Global Supply Chain Institute White Paper 2019.

[xii] Kroese*, D. P.; Brereton, T.; Taimre, T.; Botev, Z. I. (2014). "Why the Monte Carlo method is so important today". WIREs Comput Stat. 6 (6): 386–392.*

Monte Carlo methods are a broad class of computational algorithms that rely on repeated random sampling to obtain numerical results. The underlying concept is to use randomness to solve problems that might be deterministic in principle.

TECHNOLOGY IN THE SUPPLY CHAIN

THE GLOBAL SUPPLY CHAIN INSTITUTE

The University of Tennessee's Global Supply Chain Institute (GSCI) shapes and influences the practice of supply chain management (SCM) by serving as the preeminent global hub for leading practitioners, academics, and students to learn, network, and connect.

It was in this spirit of engagement and impact that the Department of Supply Chain Management and the Graduate and Executive Education programs in the Haslam College of Business at the University of Tennessee created the Global Supply Chain Institute to serve as their vehicle to extend relationships to industry and to drive an impact on the profession.

If you are interested in collaborating to better understand and advance the field of SCM, please contact us. Ultimately, we want to partner with you to help you identify your SCM strategy and develop your people.

gsci@utk.edu

gsci.utk.edu

GlobalSupplyChainInstitute

@GSCInstitute

GlobalSupplyChainInstitute

THE UNIVERSITY OF TENNESSEE KNOXVILLE

GLOBAL SUPPLY CHAIN INSTITUTE

310 STOKELY MANAGEMENT CENTER
KNOXVILLE, TN 37996
865.974.9413

GSCI.UTK.EDU