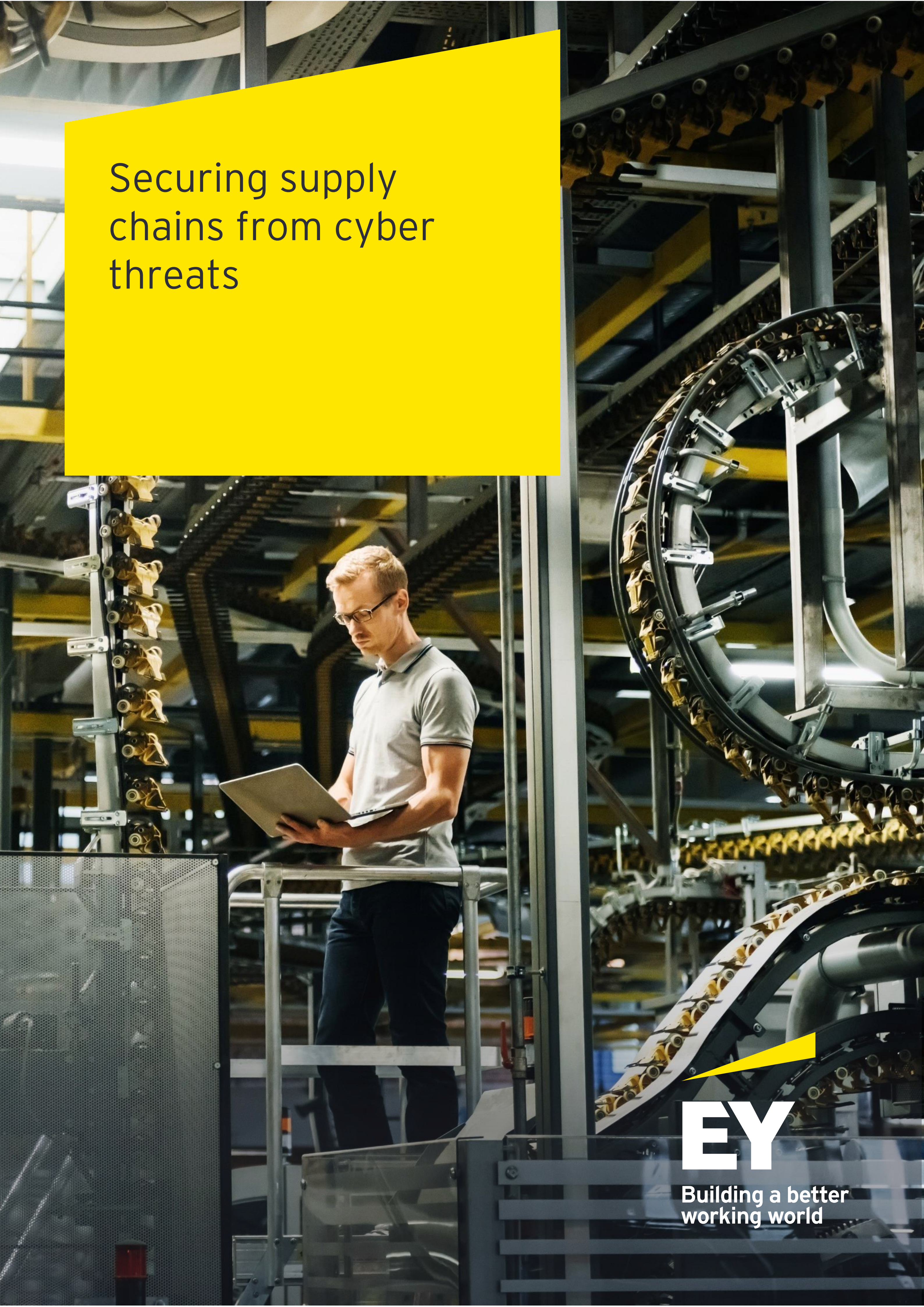
Securing supply chains from cyber threats



Building a better working world

> “
>
> In the new world of ever-connected networks and complex supply chains, building comprehensive cyber defense landscapes is vital for survival and growth.

Ashutosh Dekhne, EY Americas Global Logistics & Distribution Leader and EY Americas Leader of E2E Operations Transformations

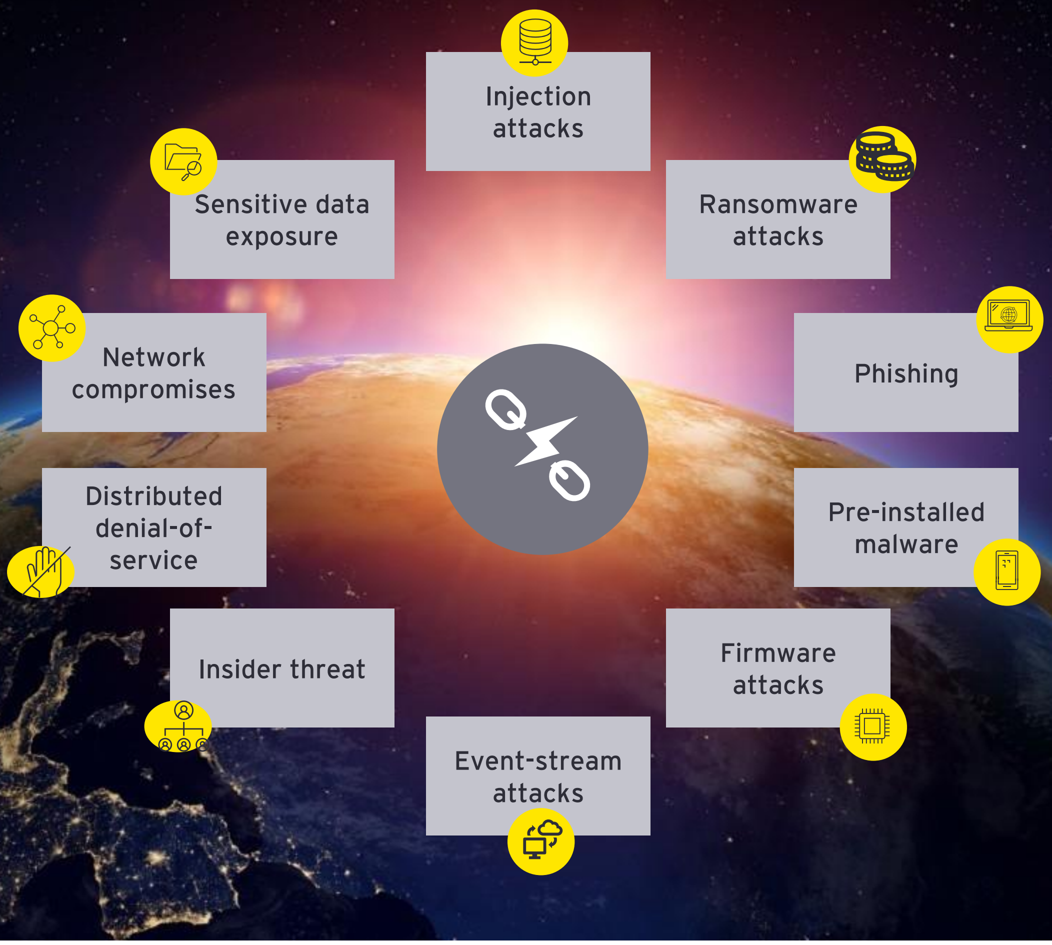
Increasing digitalization and connectivity in supply chain networks, coupled with vast amounts of data being exchanged, is making supply chains more vulnerable to cyber-attacks.

These attacks not only can result in a major financial loss for the organization but also have the potential to hurt long-standing relationships and trust among the organization, its partners and customers.

How can we modernize and build a strong supply chain capable of securing operations and increasing resiliency? Is the technology-powered new normal a secure environment to operate in? Is this transition to a digital supply network safe? These are some of the biggest questions for supply chain leaders and the C-suite in the post-pandemic world.

Still, while the supply chain is one of the highly critical functions from a business standpoint, it does not get the required attention when it comes to security against potential cyber threats. According to the EY Global Information Security Survey 2021, only 33% of chief information security officers (CISOs) are confident that they can ensure the entire supply chain is water-tight in its ability to defend against and recover from cyber threat actors. Supply chain cyber attacks can manifest themselves in different forms, as indicated in the image below. Commonly observed motivations behind supply chain cyber attacks include ransom, asset theft, service or process disruption, insider threat, and even political- or competition-driven motives.

Supply chain cyber threat ecosystem



What makes a supply chain vulnerable to cyber attacks?

With increased globalization and the rapid digital transformation of supply chains, the volume of interconnected stakeholders in the supply chain network is also increasing, resulting in higher complexity and cyber attack vulnerability for organizations. Noncompliance with cybersecurity protocols – due to a lack of training, awareness or oversight – on the part of any entity within the supply chain has the potential to cripple the cyber defense of the entire system.

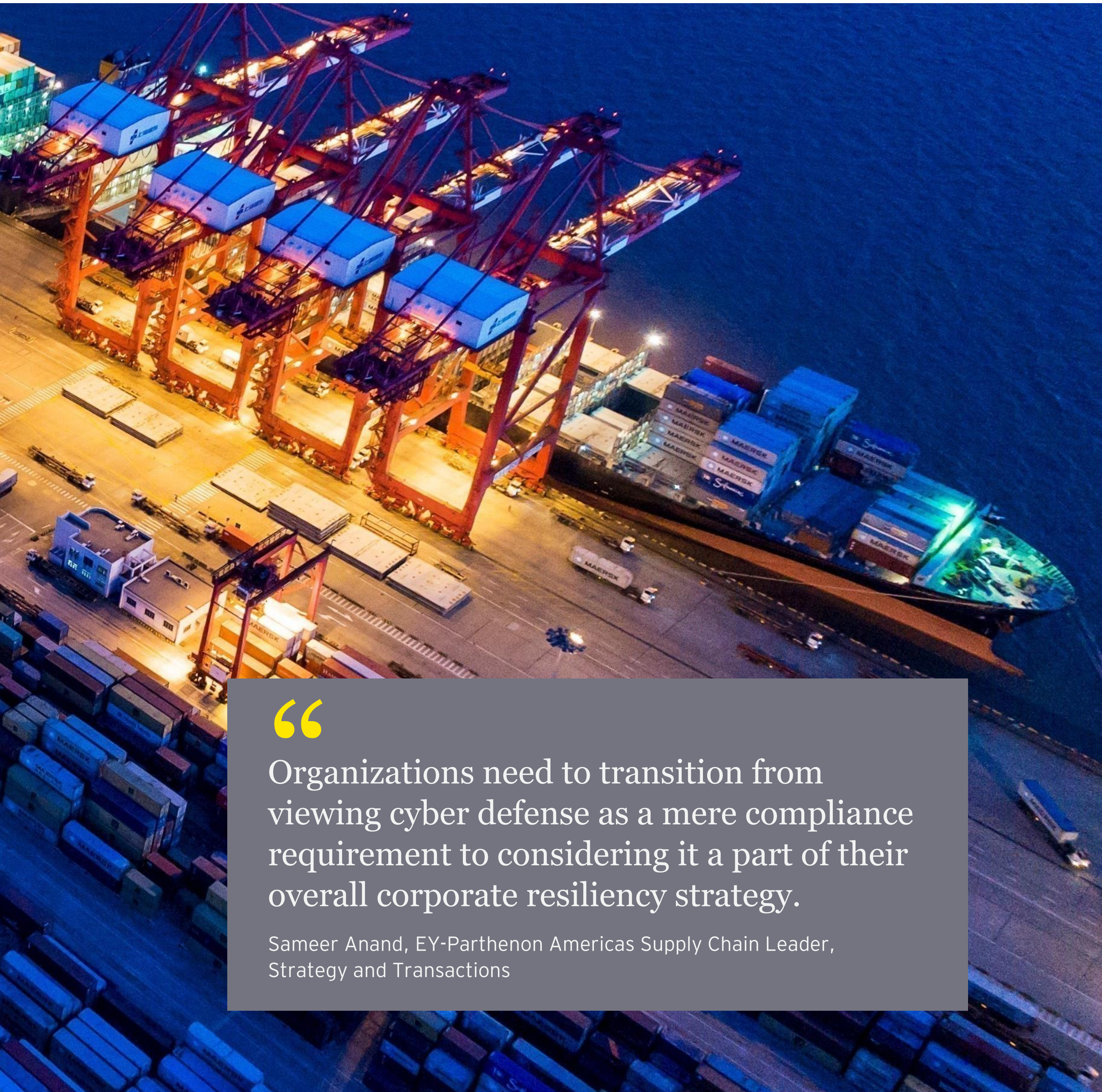
Furthermore, many parties in the ecosystem still lack a comprehensive and holistic organizational level information security strategy that can integrate information technology (IT) systems with operational technology (OT) systems, which makes every connected node in the supply chain susceptible to cyber attacks.

Why is cyber defense important?

Supply chain cyber attacks can be costly both financially and in terms of trust. For example, a medical management services company in the US suffered a supply-chain ransomware attack last year that affected over a million individuals[1] – making it one of the largest health data breaches in the US that year.

Cyber defense excellence is also emerging as a KPI influencing business engagements and strategic alliances. Now that most stakeholders view supply chain cyber defense as one of the leading contributors to business continuity, organizations with a strong cyber defense system tend to become preferred partners at every stage of engagement — vendor partnerships, distribution agreements and other strategic alliances.

Noncompliance with cyber defense mandates imposed by regulatory authorities may not only put the firm at risk of a breach but might also result in increased regulatory scrutiny, followed by fines that can also cause reputational damage. In 2021, the New York Department of Financial Services reported settlements amounting to over US$6 million in fines for cybersecurity and other related noncompliance activities.



> “Organizations need to transition from viewing cyber defense as a mere compliance requirement to considering it a part of their overall corporate resiliency strategy.
>
> Sameer Anand, EY-Parthenon Americas Supply Chain Leader, Strategy and Transactions

Which supply chain function is most vulnerable to cyber-attacks?

Involvement of technology, process complexity and third-party engagements vary at every stage of the supply chain, and so do the vulnerability to cyber attacks and the degree of potential impact on business continuity. This further highlights the need to have a carefully drafted cybersecurity strategy that addresses the gaps at each stage and builds a robust and flexible solution that can be integrated across the different moving parts of the supply chain.

Sourcing:

The ever-expanding nature of the modern supply chain, which includes multiple players and functionalities conducting high-volume data exchange, makes sourcing and procurement one of the most frequently targeted functional areas. Over the last five years, businesses have transformed digitally to leverage software-as-a-service (SaaS) for procurement and supplier management processes, which helps reduce cost and save time, but also increases data and cyber breach vulnerability, putting the suppliers' and firms' business at risk.

Enterprise resource planning (ERP) software breaches are the most prominent cyber attack type at the sourcing stage, with malicious actors targeting sensitive data at both clients' and suppliers' related to financials, customer and partner network details, invoice and order management data, account details, and other regulatory and tax evidence.

Historic attacks indicate that some of the most high-impact cyber incidents at the sourcing stage were targeted toward the supplier's system code, followed by data and internal processes. Such incidents impair operations both at supplier and client locations, thus necessitating a change of channel or supply course.

In such circumstances, clients with an internal rapid response team and an alternate supplier network are better placed to counter the operational and supply disruptions.

In February 2022, a global leader of the petroleum and energy sector announced a delay in operations and that it was compelled to reroute its oil supplies to alternate depots due to cyber attack on two of its Germany-based suppliers.

In March 2022, a Japanese multinational automotive manufacturer reported an attack on one of its key component manufacturer's IT systems, after reporting an operational halt due to a cyber attack on another major supplier in Japan in February 2022. Continued cybersecurity and supply disruptions led the firm to revise its regional production plans, cutting the output by 20% in April, 10% in May and 5% in June 2022.

Manufacturing:

Most organizations use two layers of technology: 1) IT implemented at the organization level that deals with software or hardware related to data processing and communication, and 2) OT that deals with machines, industrial control systems (ICS) and other equipment used for manufacturing and operations.

However, the two layers are not often seamlessly integrated, fuelling the potential to increase cyber vulnerabilities significantly. Manufacturing is one of the most sensitive functional domains, where a short-term cyber disruption can leave a long-term negative impact on business operations, and cost millions in downtime, lost internet protocol (IP) and inventory carrying costs.

In today's connected world, a cyber attack on a single supplier can lead to long-term suspension of manufacturing operations across multiple plants for both clients and other connected suppliers, which further leads to a chain of negative implications, such as production and distribution delays, product shortage, demand-supply mismatch, price hikes and consumer distrust.

In 2021, water and wastewater organizations in the US received a joint alert from multiple government agencies — Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA) and the National Security Agency (NSA) — regarding threats of ongoing cyber attacks that impacted ICS at water facilities. The alert highlighted risks related to data, ransomware, network segmentation, network complexity and system maintenance. It also highlighted the techniques used by threat actors to compromise IT and OT systems and networks.

Ransomware attacks leveraging cyber-incident-induced halts, remote access theft, unpatched software, ICS vulnerabilities and third-party extended network-related attacks are the most frequently observed cyber attack methods within manufacturing.

Distribution and logistics:

High dependence on third parties makes distribution and logistics one of the functions that is highly vulnerable to cyber risks. An organization, irrespective of having a strong cyber-defined ecosystem, is vulnerable if its partner firms fail to implement cybersecurity solutions with the same level of stringency. Additionally, logistics providers deal with high volumes of customer data, making them a hotspot for attackers. Data-targeted breaches are relatively higher at this stage of the supply chain. Like the sourcing process, the involvement of many highly varied participants increases supply chain complexity, making it even more difficult to implement and manage standardized supply chain cybersecurity protocols.

Additionally, the increasing use of autonomous solutions within logistics makes the function more digitally driven, further intensifying the risk of cyber attacks. In the past, attackers have also taken advantage of the ongoing rapid OT expansion, utilizing wireless communication channels as entry points to disrupt the entire supply chain. The exponential growth of logistics service providers during the pandemic has made them even bigger targets for ransomware attacks.

Recently, some of the largest global players of the shipping industry witnessed cybercrime, particularly ransomware attacks, impacting their operations for weeks — causing freight delays, exposing sensitive customer data and adding cost pressure on the firms to pay the ransom in millions.

Which sectors are most vulnerable?

Industry 4.0 has been recognized as a game changer for most sectors. As highlighted earlier, cyber attacks on the manufacturing function can have long-term impacts on business continuity, which makes semiconductors one of the most targeted sectors. Malicious behavior with the intent to access sensitive data and virtual control is another key trigger that makes sectors such as health care, consumer products, retail, automotive and energy prime targets for supply chain cybercrimes.

While the regulatory landscape varies across sectors, improving cybersecurity awareness, proactively investing in intrusion detection, monitoring and prevention tools, and implementing partner network vulnerability control frameworks to safeguard partners — especially suppliers and carriers — are emerging as top IT strategic priorities.

Sector	Extent of cyber vulnerabilities	Recent incidents
Semiconductor	The sector's linear legacy supply chain approach has evolved to introduce data-driven smart supply chain structures, driving better resource management and material flow. However, plant automation, remote working, digitalized vendor management and adoption of dynamic pricing systems include a high volume of data sharing, increasing the risk of data exposure. Between 2020 and 2022, the sector witnessed a significantly high volume of ransomware attacks, service and production disruption attacks, firmware attacks, and network compromises. Chip intellectual property theft also reported a rise, particularly during the 2021 global chip shortage period.	▶ A leading global graphics card maker reported a sensitive data exposure cyber attack.[2] The attack was trigged using unauthorized access to employee credentials **Impact: Theft of close to 1 terabyte of data, including more than 70,000 employee credentials, was reported. Further, attackers released a few product disruption-related demands that are likely to impact business performance.** ▶ In 2017, one of the top chip foundries reported a ransomware attack[3] **Impact: Production closure for nearly half a week, resulting in a revenue loss of more than US$170 million.**
Life sciences and healthcare	The volume and the criticality of products and data in this sector make it vulnerable to ransom, supply and asset theft, and sensitive data exposure threats. Although the cyber vulnerability of the sector is high, its high regulatory pressure acts as an equalizer to some extent, particularly in the US, where federal agencies have implemented acts	▶ One of the recent 2022 breaches on a leading medical group[4] in the US due to a lack of strong authorization and access systems resulted in a network compromise

Sector	Extent of cyber vulnerabilities	Recent incidents
	such as Health Insurance Portability and Accountability Act (HIPAA) to safeguard sensitive data and enact data breach reporting mandates.	**Impact: Personal data infiltration, impacting more than one million people.**
Automotive	The automotive sector is already known to be dealing with a significant volume of cyber threats such as privacy infringement, insider threats, network compromises trigged by multiple sources like phishing or pre-installed device malware, software and firmware attacks, and virtualization-as-a-malware. This is further expected to increase with the fast-evolving electric vehicles (EV) and autonomous vehicles (AV) landscape that will involve virtual- or internet-based interactivity and data exchange between millions of nodes, including the open source technology community.	▶ A leading Korean automaker recently reported a major cyber attack on its US operations,[5] resulting in a ransom demand **Impact: Nearly US$20 million worth of bitcoins were demanded in exchange for protection against data leakage. It also led to customer-facing, dealer-facing and internal IT system failure for the automaker.** ▶ In 2020, a Japan-based global automaker reported a US network compromise cyber attack,[6] allegedly induced by high-volume remote-work vulnerability **Impact: Failure of industrial control systems operations and other processes.**
Consumer and retail	Rapid expansion of omnichannel strategy, point-of-sales, and distribution management innovation; increased adoption of new business models such as direct-to-customer and buy-online-pickup-in-store (BOPIS); and more frequent use of immersive technology for both customer and partner engagements are some of the leading reasons for increased digital dependence and cyber attacks within consumer and retail sector. Some of the key motives for attackers in this sector are getting unauthorized access to data (transactional and billing data, customers' personal information, and reward and loyalty program details) and creating traffic imbalances via	▶ A global leader in meat processing suffered a network-originated cyber attack in 2021[7] **Impact: They faced operational shutdown across multiple geographies and had to release a ransom payment of more than US$10 million.** **Additionally, the site closures increased the food supply shortage threat and risked higher food prices for consumers.** **While operations could be restored timely and safely, data sensitivity became the ransom**

Sector	Extent of cyber vulnerabilities	Recent incidents
	distributed denial-of-service (DDoS) attacks.	**payment trigger during this incident.**
Energy	Reliable energy supply is of paramount importance for the day-to-day operational functioning of all sectors, including high-impact sectors such as defense and health care. This makes the energy sector extremely prone to cyber attacks. Mass service disruptions in this space could potentially trigger supply shortages and price increases and even endanger millions of lives.	▶ In 2021, one of the largest US-based fuel pipeline operators reported a ransomware attack,[8] forcing it to shut its operations, switch to a manual operations model and freeze IT systems **Impact: Disruption of service, monetary loss of US$4.4 million (as ransom), induced market shortage and panic-buying.**

How to build an effective response ecosystem against cyber attacks?

1 Organization

- Integrate cyber defense and company's resiliency strategy
- Buy insurance to cover residual cyber risks
- Streamline cyber defense budget allocation
- Conduct frequent vulnerability assessments using advanced analytics
- Implement intelligent threat detection solutions
- Converge IT-OT ecosystem
- Build a targeted talent pool and involve C-level executives in cyber defense strategy formulation stage

2 Partner Network

- Reduce risk exposure by diversifying supplier network
- Build a "Zero Trust" security architecture with vendor-agnostic solution offerings
- Use "red team vs blue team" simulation-based cyber defense strategy
- Introduce comprehensive cyber vulnerability management programs for partners
- Have a structured reporting mechanism
- Consider cyber resiliency a KPI for partner selection

3 Regulatory

- Periodically update privacy management system to accommodate regional and global level privacy laws
- Drive and support more public-private partnerships
- Transition to a more targeted compliance defense infrastructure
- Conduct cyber due diligence for every business engagement
- Assess business scenarios and monitor digital trade policies

There are several steps that companies can take to improve their cyber defense

1. Organization:

- Integrate cyber defense considerations with resiliency strategy and create a response-action contingency plan to support the same in the event of a cyber attack. This would help minimize the impact of the attack and ensure business continuity.
- Organizations can potentially opt for cyber risk and threat insurance to cover any residual risk from their cyber security program. For instance, in January 2022, one of the global pharmaceutical leaders won a legal dispute with insurers over coverage for $1.4 billion in losses from a malware-based cyberattack that it suffered in 2017.
- Focus on having a more streamlined budget allocation for supply chain cyber defense. According to EY Global Information Security Survey (GISS) 2021, 39% of respondents noted that cybersecurity expenses are not factored adequately into the cost of strategic investments, such as an IT supply chain transformation.
- Conduct system updates and frequent vulnerability assessments using advanced analytics solutions internally and across the partner landscape. Also, with the introduction of every new process and product, organizations should ensure cybersecurity and operational compliance.
- Implement intelligent security solutions to enable threat detection using historical trends and behavioral capabilities at all touchpoints. Additionally, take proactive measures to implement preventive solutions, such as the use of stronger authentication protocols and IAM (identity and access management) systems, to reduce the vulnerability of sensitive data exposure risk.
- Synchronize and converge IT systems and OT systems to ensure collaborative monitoring, timely detection, and fast-paced response to system-originated vulnerabilities.
- Invest in expanding the cyber defense talent pool by appointing a team comprising functional experts and technology experts. Also, increase the involvement of C-level executives, board members and other senior functional leaders in the cyber defense strategy formulation stage.

2. Partner network:

- Diversify the supplier base and channel strategy to potentially reduce the risk of business continuity damage, which is often caused by overdependence on a few suppliers or sales channels in the event of a disruption caused by a cyber attack.
- Build a “Zero Trust” security architecture to eliminate implicit trust and secure organizational functioning by consistently validating all digital interactions at every stage. With the increased need for remote working, companies are transitioning towards vendor-agnostic zero trust solutions to avoid passing OT system controls to a large vendor group.
- Use a “red team vs. blue team” simulation-based cyber defense strategy to establish a better prepared internal and extended network security ecosystem. As part of this approach, “red team” professionals use various techniques like penetration tests, phishing campaigns, etc., to find weaknesses in existing cyber defense systems and

processes, while “blue team” executives play the role of defensive security team protecting the organization’s systems against all cyber attacks.

- Introduce a comprehensive cyber vulnerability management program to help assess the entire partner network’s preparedness and awareness level against cyber attacks. The program should focus on risk level mapping of each vendor or partner based on the impact that a potential cyber breach could have on business continuity, along with regular monitoring and assessment of confidential data being handled by different vendors or partners.
- Develop a structured and comprehensive reporting mechanism to equip an organization to report any pre-post and simulated incident status. Further, to help evaluate investigation, containment, and recovery processes to analyze the firm and its network’s capability to assess the potential impact of cyber intrusion.
- Encourage all suppliers and other partners to consciously increase the share of cybersecurity within their respective IT budgets. Making cyber risk preparedness and cyber resiliency a KPI for partner selection might help accelerate the pace of cyber defense solution implementation across the partner network.

3. Regulatory:

- Update privacy management system to accommodate regional and global level modern privacy laws while balancing those with individual jurisdiction to standardize security protocols across the entire supply chain network.
- Foster strong collaboration between public and private entities, such as government agencies, companies, industry associations and non-profit organizations like Information Sharing and Analysis Centers (ISACs), to jointly build sector-agnostic solutions for exchanging threat intelligence in real-time and extending remedial support in case of an attack. For example, the Cyber Information Sharing and Collaboration Program (CISCP) is the Department of Homeland Security’s flagship program that enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors.

A US-based health care company built an information security team that keeps a close working relationship with peer companies, industry associations and government agencies, both to share best practices and to collaborate on effective solutions to address the increasing threats and attack methods faced by both public- and private-sector organisations.

In 2018, a leading British telecommunications firm collaborated with the UK’s National Cyber Security Centre, to launch a free collaborative online platform for sharing information about malicious software and websites with its peers to help prevent cyber crime.

- Adopt a more targeted compliance defense infrastructure by refreshing compliance protocol with specific threat-oriented mandates. For instance, in April 2022, the US Senate introduced cybersecurity legislation to manage and report ransomware payments more effectively.
- Conduct cyber due diligence for every business engagement and comply with reporting standards introduced as a part of centralized or decentralized cyber regulations. For instance, European Union's General Data Protection Regulation (GDPR) is a centralized regional guideline mandating incident reporting within 72 hours of the incident, while the US follows a decentralized approach where all states have announced their individual data breach regulations.
- Assess business scenarios and monitor digital trade policies, including tax, tariff, and duties changes, for compliance improvement and risk mitigation across the network. For instance, certain countries resort to higher tariffs as a way of deterring cyberattacks, thus making it crucial for firms to be aware and compliant with such tactical regulatory protocols.

Conclusion

The post-pandemic landscape has created a business environment where mere knowledge of cyber threats is not sufficient to run successful and protected operations. More than ever before, interconnectedness, along with large quantities of data flow, has become a part of nearly every sector — making supply chain cyber defense a priority from an operational, strategic, and regulatory perspective. Although supply chains need to be more agile and technologically powered, they also need to be secured against cyber threats that have the potential to jeopardize business continuity and hurt longstanding partner relationships and customer trust. Therefore, it is imperative for C-suite leaders and board members to increase business focus and investments in cyber defense.

[1] “Cyberattacks in healthcare surged last year, and 2022 could be even worse,” *Chief Healthcare Executive*, www.chiefhealthcareexecutive.com/view/cyberattacks-in-healthcare-surged-last-year-and-2022-could-be-even-worse, January 24, 2022.

[2] “70,000 Nvidia employees reportedly affected by recent hack,” *digitaltrends*, www.digitaltrends.com/computing/71000-nvidia-employees-affected-by-recent-hack/, March 4, 2022.

[3] “TSMC Suffers WannaCry Attack,” *PCrisk*, www.pcrisk.com/internet-threat-news/13286-tsmc-suffers-wannacry-attackx, August 7, 2018

[4] “MCG Health Faces Lawsuit Over Data Breach Impacting 1.1 Million Individuals,” *SecurityWeek*, www.securityweek.com/mcg-health-faces-lawsuit-over-data-breach-impacting-11-million-individuals, June 23, 2022.

[5] "Kia Motors America suffers ransomware attack, $20 million ransom," *Bleeping Computer*, www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/, February 17, 2021.

[6] "Honda Hacked: Japanese Car Giant Confirms Cyber Attack On Global Operations," *Forbes*, www.forbes.com/sites/daveywinder/2020/06/10/honda-hacked-japanese-car-giant-confirms-cyber-attack-on-global-operations-snake-ransomware/?sh=2153061253ad, June 10, 2020.

[7] "Meat supplier JBS paid ransomware hackers $11 million," *CNBC.com*, www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html, June 9, 2021.

[8] "Colonial Pipeline Paid Hackers a $4.4 Million Ransom," *Secior*, www.secior.com/resources/news/colonial-pipeline-paid-hackers-a-4-4-million-ransom/, accessed September 16, 2022.

Authors

Ashutosh Dekhne

Principal, Ernst & Young LLP
ashutosh.dekhne@ey.com

Sameer Anand

EY Global Retail and Parthenon
Americas Supply Chain Leader,
Strategy and Transactions
Ernst & Young LLP
sameer.anand@parthenon.ey.com

Tony Sibert

Managing Director,
Ernst & Young LLP
tony.sibert@ey.com

Anthony Mubarak

EY-Parthenon Senior Director
Strategy and Transactions
Ernst & Young LLP
anthony.mubarak@parthenon.ey.com

Demi Burton

EY-Parthenon Director
Strategy and Transactions
Ernst & Young LLP
demi.burton@parthenon.ey.com

Mukta Gupta

Senior Manager, EY Global Delivery
Services India LLP
mukta.gupta@gds.ey.com

Sudhanshu Wasan

Manager, EY Global Delivery
Services India LLP
sudhanshu.wasan@gds.ey.com

Runjhun Anurag

Assistant Manager, EY Global
Delivery Services India LLP
runjhun.anurag@gds.ey.com

2208-4086829
US SCORE no. 17082-221US
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global EY organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com