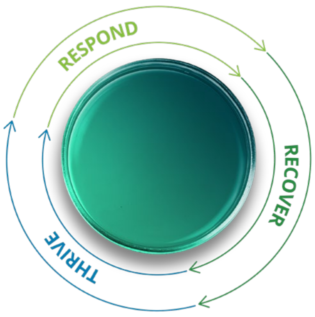
Deloitte.



The rise of cyber threats to supply chains amid COVID-19

A weekly high-level brief that focuses on some of the most current cyber threats and trends as identified by Deloitte Cyber Threat Intelligence (CTI), with near-term recommendations on managing cyber risks to respond, recover and thrive through the COVID-19 global pandemic.

#5| May 2020

Growing cyber threats amid COVID-19 can be a menace to supply chains

4 in 10 Manufacturers

Surveyed indicated that their operations were affected by a cyber incident in the past 12 months*

Between 2017 and 2018 cyber incidents increase by

3.5x Ransomware
2.5x Spoofing
0.7x Spear-phishing

Manufacturing industry consistently featured among the most frequently targeted industries

Major cyber risks

87% Unauthorized access

86% Operational disruption

85% Intellectual property theft

$330,000 Average financial impact from an IoT-focused cyber incident

$7.5M Average financial impact from a data breach in 2018

In the past 60 days, there has been an increase in attacks to supply chain related to COVID-19, including targeted attacks on known organizations (e.g., UPS). Defining security requirements and having a cyber-risk management program to evaluate third-party (and even fourth-party) services can help organizations reduce the risk of attacks on their supply chains. In supply chain, we have multiple vendors who communicate to each other through email. In Early April 2020, the FBI released a statement indicating an anticipated rise in Business Email Compromise (BEC) schemes related to the COVID-19 pandemic. Business Email Compromise attacks exploit these relationships to trick one or more vendors into wiring money to the malicious attackers. According to the FBI, BEC attacks cost organizations approximately $1.77 Billion USD in losses in 2019. Companies conducting business with foreign entities are more susceptible to BEC attacks as their employees might fail to recognize unusual business behavior exhibited by a foreign supplier.

Cyber vulnerabilities in supply chain are on the rise

Gaining a better understanding of how supply chains are changing in light of this global pandemic could help retailers and other businesses secure, adapt, and move ahead following this incredibly difficult period. In 2019, 40% of manufacturers had their operations affected by a cyber incident. With supply chains already facing risks of shutdown, reduced operations forward in these due to social distancing, and re-tooling operations to make Personal Protective Equipment, additional disruptions from cyber incidents may have a more severe impact. **This week we highlight the rising threats targeting elements of supply chain** (and originally identified in our detailed threat report dated April 22 – April 28).

Phishing campaigns impact our well-known shipping companies

Impact reach: All| Geographies: Global

In April 2020, Deloitte CTI observed two phishing campaigns and one malware using COVID-19 lures. These COVID-19 phishing campaigns impersonated well-known shipping companies such as FedEx, DHL, and UPS, as well as, targeted US-based medical providers with malicious attachments.

Business Email Compromise (BEC) result in fraudulent financial transfers

Impact reach: All| Geographies: Global

On April 15, 2020, Deloitte CTI observed multiple spam campaigns against businesses conducting Business Email Compromise attacks using Coronavirus (COVID-19) themes. In these attacks, the attacks used COVID-19 themed emails such as payroll, wire transfer, or legal attention social engineering themes requesting their targets make fraudulent financial transfers.

The root cause | Mitigating risk in Operational Technology (OT) environments during the time of COVID-19

As many leading manufacturers raced globally to do their part to produce critical COVID-19 supplies such as personal protective equipment and ventilators, even new vaccines, they may become targets of theft or extortion by cyber adversaries looking to exploit vulnerabilities that could lead them to valuable intellectual property. The potential for damage in an operations environment can dramatically affect revenue and may shut businesses down completely. Managing risk across an extended supply chain is often challenging. For large companies, there might be thousands of different third, fourth, and fifth parties that they have to consider. Whether it's a supplier that embeds something into a subcomponent, or a software product. With more connected components, communicating and storing data, the risk rises, and the attack surface is expanded. This time of uncertainty caused by the novel coronavirus has shown us that we aren't quite as prepared for "anything" as we thought. There are many areas where people, process, and technology overlap between the IT and OT ecosystems. The below highlights the top cyber concerns that manufacturers should be aware of as they look to converge IT and OT across their operations.

OT system characteristics*	Cyber concerns
The complexity of IT and OT convergence	• OT is typically managed by engineering, automation, and operations rather than IT. • There is generally no single team responsible for all OT systems and underlying security. • Traditional application of security controls such as patching or vulnerability scanning cannot usually occur without detailed evaluation. • Deep knowledge of the industrial processes, technology assets, network architectures, risks, and security approaches are often essential, leading to the need for integrated teams across both IT and OT working together.
Update paradox	• No single approach for patching or updating systems is possible. This can make it difficult to be responsive when vulnerabilities are detected, often driving the need for defense-in-depth approaches to be adopted.
Legacy system setbacks	• Many systems have long life cycles (10+ years) and were not built to be externally connected. With the increase in edge computing, cloud platforms, and the adoption of other smart factory technologies, air gapping is no longer a viable option.
Destabilized infrastructure	• Older equipment often uses proprietary communication protocols that can be easily disrupted if data communication within the network segments increases. • Existing networks and associated architectures were not designed to handle the data flows required for the adoption of these new technologies. • There are limited vetting processes to understand the security risks associated with new technologies being acquired and deployed – increasing the risk of an attack affecting both this new technology and other legacy technologies on the same networks.
Operational constraints	• Real-time capabilities are typically essential; introducing additional security controls could introduce latency. • Making network or other changes could require downtime or an outage. Downtime due to maintenance should be limited to absolute minimums. • Software updates are often not possible due to the proprietary nature of products or contracts or equipment age. • Establishment of clear responsibilities across functions (IT and OT) can be crucial. It is important to approach addressing cybersecurity risks using cross-functional teams, considering what each group does well.

*Source: Cybersecurity for smart factories

Recover and Thrive | Securing supply chain for the “next normal” – Spotlight on smart factories

As manufacturing organizations evolve processes and protocols amid COVID-19, they should invest in a holistic cyber management program that extends across the enterprise (IT and OT) to identify, protect, respond to and recover from cyberattacks. Specifically, the following four steps should be considered when starting the process of building an effective manufacturing cybersecurity program:

Perform a cybersecurity maturity assessment on new technology developed. With every new use case in pilot or production within the smart factory, there come new exposures to threats. The assessment should include OT environments, business networks, and advanced manufacturing cyber risks such as IP protection, control systems, connected products, and third-party risks related to industrial ecosystem relationships.

Establish a formal cybersecurity governance program that considers the evolution of OT in response to COVID-19. Business-centric representation in these governance structures is important to allow IT and OT teams to collaborate where practical and manage the business. The manufacturing security teams should work closely with the site to consider the risks and appropriate mitigation strategies.

Prioritize actions based on risk profiles and demand amid COVID-19. Use the results of the cybersecurity maturity assessment to create a strategy and roadmap that can be shared with executive leadership and, where appropriate, the board to address risks that are commensurate with your organization’s risk tolerance and capabilities.

Build in security to COVID-19 related technology transformation. Since many smart factory use cases are still in planning and early stages, now is the time to harmonize these projects with your cyber risk program. Design and include the appropriate security controls at the front end of these projects. Important controls to consider include use of secure network segmentation models, deployment of passive monitoring solutions, secure remote access, control of removable media, improved management of privileged access, and executing consistent backup processes.

We’re by your side to help you through COVID-19

Relevant Deloitte reads:

- On-Demand Webcast: Responding to COVID-19 with business resilience, trust, and security
- Article: Ransoming government
- Article: COVID-19 response capabilities for health care organizations
- Article: The heart of resilient leadership: Responding to COVID-19

Deloitte Cyber helps organizations perform better, solving complex problems so they can build confident futures. Smarter, faster, more connected futures—for business, for people, and for the planet. As a recognized leader in cybersecurity consulting, Deloitte Cyber can help better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen our clients’ ability to thrive in the face of cyber incidents. Deloitte Cyber uses human insight, technological innovation and comprehensive cyber solutions, to manage cyber everywhere, so society can go anywhere.

Deloitte China Cyber Risk Partners

Xue, Tonny
National Cyber Risk Leader
Tel: +86 10 8520 7315
Email: tonxue@deloitte.com.cn

Feng, Steven Ye
Eastern Region
Tel: +86 21 6141 1575
Email: stefeng@deloitte.com.cn

Kukreja, Puneet
Eastern Region
Tel: +86 21 3313 8338
Email: puneetkukreja@deloitte.com.cn

Jiang, David Wei
Eastern Region
Tel: +86 21 2312 7088
Email: davidjiang@deloitte.com.cn

Shih, Nathan Pei-en
Eastern Region
Tel: +86 21 3313 8366
Email: nathanshih@deloitte.com.cn

Zhang, Boris Zhen
Eastern Region
Tel: +86 21 6141 1505
Email: zhzhang@deloitte.com.cn

He, Tommy Xiaoming
Northern Region
Tel: +86 10 8512 5312
Email: the@deloitte.com.cn

Xiao, Frank Tengfei
Northern Region
Tel: +86 10 8512 5858
Email: frankxiao@deloitte.com.cn

He, Vivi Wei
Southern Region
Tel: +86 755 3353 8697
Email: vhe@deloitte.com.cn

Kwok, Eva Yee Ngar
Southern Region, Hong Kong
Tel: +852 2852 6304
Email: evakwok@deloitte.com.hk

Pihkanen, Miro
Southern Region, Hong Kong
Tel: +852 2852 6778
Email: miropihkanen@deloitte.com.hk

Ma, Luke Kwok Kwan
Southern Region, Hong Kong
Tel: +852 2852 1086
Email: lukema@deloitte.com.hk

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Shanghai, Singapore, Sydney, Taipei and Tokyo.

The Deloitte brand entered the China market in 1917 with the opening of an office in Shanghai. Today, Deloitte China delivers a comprehensive range of audit & assurance, consulting, financial advisory, risk advisory and tax services to local, multinational and growth enterprise clients in China. Deloitte China has also made—and continues to make—substantial contributions to the development of China's accounting standards, taxation system and professional expertise. Deloitte China is a locally incorporated professional services organization, owned by its partners in China. To learn more about how Deloitte makes an Impact that Matters in China, please connect with our social media platforms at www2.deloitte.com/cn/en/social-media.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.