IL2000

HOW TO MITIGATE THE RISK OF SUPPLY CHAIN CYBERATTACK

How to mitigate the risk of supply chain cyberattack

Right now, over 50 billion internet-connected devices are scattered across the planet. As of 2020, each of the 7.75 billion people (and change) living on this space rock generate an average of 1.7 megabytes of data every second. If you're into metrics, that's the data equivalent of Tolstoy's 1200-page masterpiece, War and Peace, every second.

Data soaks into every corner of life, including our vast global supply chain, whose smooth running relies on an intricate planet-spanning web of connectivity. While the efficiency gains are hard to overstate, alongside this digital revolution we're seeing a sharp increase in supply chain cyberattacks.

In the last year alone, supply chain attacks have increased by over 400%. Gartner estimates that 45% of organizations worldwide will have experienced a cyberattack on their supply chain by 2025, an astounding statistic when you consider that this figure hovered in the low teens in 2021. We're emerging into a time of unprecedented supply chain security risk.

Unique challenges

Just a few years ago, many supply chain-dependent companies could get away with tackling cybersecurity as part and parcel of their overall cyber risk reduction posture.

That's no longer the case.

By definition, supply chains are about connectivity: one point in a node links to another, then another, branching out across sprawling pathways of organization that span companies, technologies and oceans. Distribution hinges on open pathways and ease of access.

The problem is that any infrastructure built to optimize communication and data flow presents an ideal environment for cyberattacks. The headlines over the last few years have been filled with examples of transportation and logistics companies falling prey to devastating attacks on their data and communication infrastructure.

Targeted response

Any company with a freight operation will soon reach a point where it needs to develop a comprehensive and targeted approach to online supply chain security

That approach requires more than mere financial investment. It'll take a mind shift, an institution-wide acknowledgment that supply chains aren't just vulnerable at computer terminals. The approach will encompass not just computer terminals but merchandise scanning equipment, warehouse machinery, vehicles, and a long list of other connected tech.

Contents

This white paper synthesizes three overlapping fields of knowledge — data security, supply chain risk analysis, and supply chain optimization — to present an objective and accurate picture of supply chain cybersecurity in a post-Covid world.

Areas covered include:

- **The 2022 supply chain cybersecurity outlook:** An overview of the main moving parts that shape supply chain cybersecurity today.
- **Recent case studies:** A description of three data breach incidents that have shaped supply chain security analysis. Spanning a small trucking operation to an enormous multinational logistics company, these case studies serve to illustrate some of the more important dimensions of risk as well as the lasting repercussions of a successful data breach.
- **Principles of best practice:** An overview of the principal aspects of best practice in supply chain cybersecurity, covering fundamentals, technology and systems, people management, organizational partnerships, and governance. In each of these areas, the paper offers useful resources for further research.
- **Future-proofing challenges:** A brief foray into some emergent cybersecurity issues that look set to shape supply chain security in the years to come.

The supply chain cybersecurity outlook in 2022

Over the last few years, we have seen an explosion of new technologies and new threats. Following are some of the main factors shaping supply chain cybersecurity today.

More incentives

The incentive to technologically innovate is stronger than ever. The World Economic Forum estimates that the digitalization of the global marketplace will unlock $1.5 trillion in new business opportunities for logistics providers by 2025.

The race is on to build faster, more agile systems for moving products. To keep up, logistics providers and logistics-dependent companies will need to invest in new technologies, the corollary being heightened exposure to risk.

Growing threats

Where opportunities grow, threats grow too. There has been a huge surge in cyberattacks, most notably ransomware attacks. These affect everyone, from small businesses with a small online profile to enormous companies with sophisticated systems.

Beyond the costs of system restoration, a successful ransomware attack is often devastating to business continuity. A typical attack will cost a logistics company millions of dollars in downtime, with substantial reputation damage following in its wake. To avoid these consequences, many firms are capitulating to ransomware demands – an understandable response but one that incentivizes future attempts.

Analysis of recent attacks suggests that supply chains are rapidly becoming a focal point for malicious online actors. In 2021, two-thirds of reported breaches in the US resulted from vulnerabilities in supply chain systems according to a recent national threat assessment.

Greater complexity

Logistics-dependent companies are fighting a battle on multiple fronts. There are more attack surfaces than ever before.

Digital transformation has revolutionized supply chains. Warehouse robotization, automated transport, and the increasing role of AI – to name just a few pivotal technologies – are making supply chains faster and more efficient, but they all present new and overlapping operational technology (OT) vulnerabilities.

At the same time, companies are having to pay far closer attention to the security of the transportation management software (TMS) they use. In the surge to build bigger, better systems, coding is becoming increasingly distributed. Software-focused logistics providers are taking shortcuts, outsourcing coding tasks to the freelance marketplace. In a 2021 analysis of software supply chain risk mitigation, Gartner recommends that security hygiene "should now extend to external code dependencies and commercial off-the-shelf software."

In 2022, companies with complex freight operations face considerable software uncertainty. Managers and technicians making software decisions are aware that they need a way to thoroughly vet the security of their systems, but they're unsure of how to systematize that approach or even of what questions to ask.

The social backlash

As all these uncertainties unfold in the corporate and technical spheres, society is watching on. The news cycle has had its fair share of horror stories where a cascade of cyberattacks leads inevitably to private data being stolen, captured and exploited.

Just as growing ecological awareness has, in past decades, pressured the private sector to enshrine greater resource accountability into production practices, companies are paying closer attention to a society-wide acknowledgment of a collective responsibility to keep data safe.

Regulatory fallout

The US government is mounting a more aggressive and focused response to successful cyberattacks. The US Department of Justice and the FBI's recent involvement in seizing $2.3 million of extorted funds from ransomware cybercriminals is just one example of a growing crackdown on ransomware.

As an extension of this heightened law enforcement effort, supply chain operations will likely face tighter regulatory requirements. Fines for data breaches are already considerable if they impact PCI, HIPAA or FedRAMP regulations. Companies may soon need to tackle additional compliance requirements to safeguard their supply chain operations.

The bottom line: We aren't ready

While cybersecurity has focused extensively on IT security for some time now, securing operational technology (internet-connected machinery and devices) is in its nascence. Most businesses aren't ready for the cybersecurity implications of the rapidly digitalizing global marketplace.

Case studies

This section describes three recent supply chain data breach incidents. Spanning a small trucking operation to an enormous multinational logistics company, these examples illustrate some of the key dimensions and critical repercussions of a successful data breach.

Small trucking company

One morning, a small business owner received an email. The anonymous sender gave an ultimatum: pay a ransom of $300,000 or have all the company's sensitive data leaked to the public. Attached to the email were screenshots captured directly from the company's TMS.

The cybercriminal's threat to leak confidential customer data was alarming enough, but the owner of this small, 25-truck transportation operation realized the threat ran deeper than that. Armed with the ability to see inside the company's operation, the unknown hackers could, if they wished, disrupt the movement of trucks and freight. The final crippling blow came when the company owner realized the ransomware attacker had encrypted much of the company's data. The files still existed on the company's server, but the data could only be unlocked with a password.

Overnight, the trucking company found itself facing three overlapping threats:

1. A leak that could cause severe damage to the company's reputation and good standing with clients.
2. A tangible public liability and safety issue given that the company's fleet of trucks could be influenced by the hacker's control over management systems.
3. The sudden inability to access critical operations data.

Interviewed by FreightWaves, the business owner relates his initial reaction, which was shock that a small company like his was targeted for attack. The company didn't pay the ransom. Their data was leaked as the ransomer had promised and there was a period of intense uncertainty for the company. The company was eventually able to return to business as usual, albeit with much stronger cybersecurity measures in place.

Large-scale transport operation

This successful cyberattack happened to a Wisconsin-based transport company. A major carrier for the region, the business ran a fleet with over 3000 drivers. In early October of 2021, its busy operation ground to a halt, FreightWaves reports, when the company's proprietary online operating system — essentially the nerve system of its transportation operation — suddenly ceased to function.

Logistics personnel found themselves unable to send rate confirmations or track loads, giving the company no choice but to temporarily shutter a major part of its business until it could regain access to its data. Soon afterward, data stolen from the company appeared on a prominent ransomware gang's leak site.

While a complete report of this attack has not been released by the company, the evidence (available in part from their October 2021 SEC filing) paints a familiar picture of established ransomware methods:

1. A public and embarrassing announcement that the company's data has been stolen, along with proof.
2. Encryption of critical company data — in this case, the gang alleges over 100 gigabytes worth — leading to prolonged business disruption.
3. Significant legal and public relations repercussions of data theft. In this case, employee data was stolen, and the company undertook to offer "identity restoration services at no cost for two years."

Global logistics company

As proof that cyberattacks can happen at any scale, this successful cyberattack happened to a Fortune 500 logistics company with headquarters across 100 countries, a workforce of over 18,000 employees, and assets totaling more than US$3 billion.

The attack likely occurred in February of 2022 and, on this occasion, targeted only a critical subsection of the company's enormous infrastructure of systems. "Systems impact related to the cyber-attack limited our ability to arrange shipments or manage customs and distribution activities, or to perform certain accounting functions," the company's CIO said in a public statement soon after the attack.

The fallout was extensive:

1. The company is estimated to have lost $40 million in failed delivery charges, with key services disrupted for three weeks after the initial attack.
2. In the weeks that followed, all their core services were temporarily taken offline to protect other systems and data from damage and theft.
3. The company outlaid an additional $20 million on full system recovery after the attack.

The initial threat vector that caused these shockwaves of disruption through the company has not been revealed.

What do these case studies reveal?

- You can't be too small or too large to be at risk and the risks can be costly.
- Targets are typically critically unprepared and have no strategies in place to respond swiftly and decisively. There's a critical period of chaos and uncertainty where decisive action might have mitigated the impact.
- Reputation damage is a critical risk. 41.5% of companies disrupted by a supply chain cyberattack experience a deterioration of trust from their customer base, according to one 2022 analysis.
- The liability implications are enormous. Attacks often expose a company to the risk of causing significant harm to the public, or to public and private infrastructure. An effective legal response is therefore vitally important.
- A prevention plan isn't enough. Supply chains are complex and multifaceted, and cybercriminals constantly seek to find new exploits. A mature strategy is one that has a response plan in place as well as a prevention plan.

Principles of best practice

Here we provide an overview of the principal aspects of best practice in supply chain cybersecurity, covering fundamentals, technology and systems, people management, organizational partnerships, and governance. While these principles set a strong foundation for supply chain cybersecurity prevention and preparedness, each company faces its own unique security considerations and should plan accordingly.

The fundamentals

The fundamentals of general cybersecurity practice still apply at the supply chain level. The National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity provides an excellent overview, categorizing preparedness across five categories:

1. Identify

Understand and quantify the risk to systems, people, assets, data and capabilities. An important starting point is maintaining a centralized inventory of infrastructure and assets that have "smart" or Internet of Things (IoT) capability. The complexity here is that not all connected devices are obvious. Additionally, maintain basic systems for asset management and clear governance structures around maintenance and access.

2. Protect

Build safeguards that protect the delivery of critical services. At a minimum, this requires that a secure identity management system be implemented. While good data practice is often observed across computer terminals, identity management for internet-enabled equipment and vehicles is frequently overlooked.

One significant vulnerability inherent in early generation IoT devices is that they come pre-configured with default passwords, all of which should be amended to secure and unique passwords. Data security specialists are increasingly recommending that transport and logistics enterprises implement "zero trust" protocols across their networks — a system where authentication is required both within and outside network architecture.

3. Detect

Establish robust systems and protocols to identify cybersecurity attacks. For larger operations this may entail continuous, round-the-clock monitoring. At the very least, network security software should monitor traffic and report on suspicious behavior.

4. Respond

Many businesses still exhibit slow or minimizing responses to cyberattacks, even successful ones.

Beyond eliminating the immediate threat, transport and logistics companies should conduct formal response planning, mount a concerted legal response, analyze the attack vector to eliminate future vulnerability, and communicate effectively with stakeholders who may also be affected by the data breach.

5. Recover

Have a plan in place to maximize resilience after an attack. Recovery planning should encompass systems development to maintain data security on an ongoing basis and public relations to mitigate reputation damage.

Technology and systems

Technology and systems should be developed with an eye for simplicity and clarity.

1. Simplify digital infrastructure

Whether it's a computer or another internet-enabled device, a general rule of thumb is that the more complicated it is, the easier it is to exploit. "With the rapid adoption of cloud computing and the Internet of Things (IoT), the supply chain has many new entry

points and attack surfaces for cybercriminals to infiltrate," the Director of AT&T Cybersecurity, Bindu Sundaresan, warns in an article about supply chain risks for Inbound Logistics.

The same rule applies to IT solutions. "To enhance the customer experience and ensure brand consistency, transport and logistics companies are using omnichannel marketing approaches such as onboard internet access, customer portals, real-time status tracking and touchless payments. Although these new marketing strategies benefit customers, they risk introducing new threat vectors that attackers can use to compromise systems," according to security advisor Fortinet.

Digital transformation imposes an impetus toward "feature-bloat" solutions, a push exacerbated by the tendency of third-party logistics service providers to offer software-only solutions. Consider simplifying your systems to fewer providers, preserving only those functions you actually use.

2. Know who has access

According to a 2018 inventory data access survey, only a little over a third of companies maintain a centralized list of third parties with whom they share information. Somewhat ironically, a concurrent survey conducted by cybersecurity analyst, RiskRecon, found that almost a third of companies have vendors they suspect may pose a significant data breach risk.

It's easy to lose sight of how your technology is networked. The addition of one new logistics-related technology can radically change a company's vulnerability to supply chain disruption.

In its 2022 report on best practices in supply chain risk management, manufacturing advisor ThomasNet recommends regularly auditing your digital infrastructure to maintain an accurate snapshot of who can access your data, what they do with it, and who they're sharing it with.

3. Identify risks introduced by third-party products

In its 2021 analysis of software attacks on supply chains, Gartner found that malicious code injection during software development was a significant underlying factor in many supply chain attacks. This further reinforces the need for awareness not just of who is using your software but who is *developing* it too.

The National Institute of Standards and Technology sets a high bar, recommending that an IT professional analyze source code for all new software entering a company's digital ecosystem. While appropriate for some operations, this is likely beyond the capacity of many transport and logistics companies. At a minimum, however, it's advisable to ask questions and ask software developing houses for proof that their products handle data safely.

People

No system exists in isolation from the people who run it. Protecting a supply chain's resilience relies on well-trained and informed human operators.

1. Train your staff

"Cybersecurity is never just a technology problem; it's a people, processes and knowledge problem (NIST)." People present the greatest vulnerability in most computerized systems.

Just one mistakenly opened email can introduce malware into a computer network. One shortcut when onboarding new machinery can leave critical exploits wide open across a company's whole infrastructure. Just one carelessly placed password can cost a company millions of dollars.

It's therefore vital to train all logistics and transportation staff in security practices. Almost every security professional in the space places particular emphasis on training personnel to identify phishing attacks. They remain one of the more common human errors preceding a data breach.

2. Gain an outside perspective

As the case studies in this paper illustrate, a company may be broadly aware of security issues and yet unable to see the threat. The biggest danger is the thing one doesn't see coming. Whatever a business's size, it's prudent to have a security expert appraise its cybersecurity posture. Moreover, tasking a third-party logistics expert to analyze a supply chain for critical vulnerabilities is likely to yield insight into

additional and possibly interrelated vulnerabilities.

Partners

Supply chains are densely networked chains of cause and effect. A business is only as secure as its least secure partner.

1. Partner with secure companies

In 2020, a ransomware attack on a Canadian trucking company swiftly led to a string of attacks on companies in adjacent industries. This caused security analysts to believe that critical data on these companies had all been stolen from the same source. Who a company partners with can have a profound impact on its exposure to risk.

Yet companies consistently fail to monitor this risk. In a 2022 study on supply chain resiliency, security consultancy Interos found that only 11% of companies continually monitor the security of supplier freight operations. Over a third reviewed their exposure to risk on a monthly or quarterly basis.

Companies can lay the groundwork for secure supply chain partnerships by investing in business intelligence tools capable of delivering real-time visibility over freight activities. Additionally, the National Institute of Standards and Technology advises companies to systematically train vendors in security requirements and to build a training requirement into every RFP and contract.

However operationalized, it's vital to partner with companies that care about security as much as you do. At IL2000, we recognize that we are guardians of your profitability, and that means we're guardians of your data. That mindset guides everything from system development to daily data handling practice.

2. Work with the right 3PL

Working with a third-party logistics provider can tangibly strengthen a company's security position. A good 3PL supports secure system infrastructure for sharing supply chain data. An excellent 3PL can also provide real-time updates on shipping irregularities and foster secure supply chain operations with a team of experts skilled in identifying and mitigating risk.

However, as with any data-sharing partner, a company is only as secure as its 3PL. If the 3PL's digital assets aren't safe, neither is the data of its clients. Therefore, it's good practice to review the software architecture upon which a 3PL's transportation management system is built. Crucial questions include:

- **Do they own the software they sell? Did the 3PL develop it?** As previously discussed, it's standard practice for software developers to outsource much of their coding to unknown, unvetted coding houses. This practice opens a door for cybercriminals to hard-code vulnerabilities into software that they can exploit later. A company should make sure that its 3PL owns and developed its own software.
- **Can the 3PL's systems be customized to clients' needs?** Two of the three case studies in this paper describe a cyberattack that originated with human error. Human fallibility remains the greatest exploit in any IT or OT product. The more customized and structured a company's TMS solution is to its daily operations, the greater the likelihood its data will be well-maintained and properly managed. Every instance of IL2000's proprietary TMS is closely tailored to clients' data requirements, and this paves the way for a secure, well-maintained data set.
- **Is data shared via a secure and trusted service?** A factor that will have a significant bearing here is whether the TMS software is client-server or cloud-based. While both models have advantages, from a physical security standpoint, the advantage of a cloud-based solution is that this passes the risk of physical access to data to the cloud computing provider, who will be required to conform to the highest security standards.
- **Is the 3PL software equipped for disaster recovery?** A mature security posture acknowledges the importance not just of prevention but also of recovery. On average, it takes a company 197 days to identify a breach and an additional 69 days to bring it under control, cybersecurity firm Varonis reports in its 2020 analysis of data breach response times. Companies that can shorten this response time down to 30 days save over a million dollars on average, IBM reports. It's prudent to gain a sense of how quickly your 3PL can recover your data in

the event of a breach and how frequently data snapshots are securely stored.

Governance

Cybersecurity doesn't just happen at an operational level. It starts with strategic and financial decisions in the board room.

1. Invest in cyber liability insurance

Some 78% of corporate risk managers purchased cyber liability insurance in 2020, according to Investopedia. That's up from just 34% in 2011. Insurance is a vital requirement for companies managing medium to large supply chains, particularly given the risk and potential consequences of a supply chain cyberattack.

Consider the case of Colonial Pipeline, where hackers were able to undermine the supply of vital fuels across much of the United States. The company had no choice but to pay the $5 million ransom without cyber insurance.

2. Mainstream IT into corporate governance

"Gone are the days of 'this is an IT problem.' It's every business leader's problem to solve," AT&T's cybersecurity director said about supply chain security in an article for Inbound Logistics.

It's not unusual for even large companies to relegate IT to the decision-making basement. These departments are frequently seen as filled with technicians not strategists. Business leaders and IT leaders need to work together to acquire a more nuanced picture of how business goals and enabling technologies collide. IT decision-making needs to find its way to the board table.

Future-proofing supply chain cybersecurity

Cybersecurity threat assessment is a moving target, especially in relation to supply chain management, a process dependent on a wide array of rapidly evolving technologies. Adopting best practice today means future-proofing your cybersecurity strategy against what's coming next. This section speculates on some of the more significant emergent challenges for cybersecurity.

The digital dimensions of counterfeit

Counterfeit supply chains cost US manufacturers over $130 million in 2021.

Historically, we've thought of counterfeit as a conventional security issue rather than a cybersecurity issue, but that's changing. A cybercriminal can now modify product details electronically. They can amend expiration dates. They can even apply a genuine electronic tag to a non-genuine product. And all of this occurs digitally.

Counterfeit is likely to affect more businesses in the near future, and in unpredictable ways.

Over the next few years, preventing counterfeit looks set to be about ensuring digital security all along the supply chain. Logistics companies and manufacturers may embrace the rapidly maturing field of supply chain blockchain technologies to build "an immutable digital ledger and transparent exchange of electronic information" to track goods as they travel from location to location.

As the trajectory of the global counterfeit crisis illustrates, the line between cybersecurity and conventional security is blurring.

A more data-driven approach to third-party risk management

By 2025, Gartner projects that 60% of US organizations will use cybersecurity risk as a deciding metric and determinant for their third-party transactions.

In the past, companies have relied on imprecise methods when defining third-party risk. Questionnaires are frequently employed. Some companies even rely on gut feel when quantifying risk introduced by sharing data with partner companies. Based on the results of a 2020 survey on third-party risk management, RiskRecon found that only 34% of decision-makers believed subjective responses were accurate and truthful.

The growing interconnectedness of data coupled with the heightened sophistication of cyberattacks makes this approach too imprecise. With the stakes as high as they are, companies will increasingly turn to third-party risk programs to provide rigorous and data-driven insights into vulnerabilities introduced by working with third parties.

The technical inertia of legacy IoT equipment and operational technology

The Internet of Things is no longer a new phenomenon. What started as a technological frontier has matured into more robust technology purpose-built for a vast range of consumer and industrial needs. While new devices appear in workplaces, older generation tech remains in operation.

"Some industrial control system devices in the field operate for decades after they are deployed," threat intelligence firm Fortinet reports. The further we move into the age of IoT capability, the greater the technical debt companies will experience maintaining these diverse layers of technologies. In the coming years, companies may experience a kind of technical inertia where they struggle to maintain visibility across older systems and equipment.

Increased societal pressure to adopt a comprehensive cybersecurity posture

"Cybersecurity is turning into a social phenomenon (Gartner)." Investors, customers, and the public at large are becoming increasingly aware of the personal and social threats a data breach imposes. There's a growing public expectation that companies should track and report against cybersecurity benchmarks.

From executive performance evaluations to consumer watchdogs keeping score on how effectively businesses can maintain the integrity of their systems, we can expect the future to place higher expectations on people and organizations alike.

Supply chain cybersecurity and the thin digital line between opportunity and threat

Over the last few years, the emerging landscape of technology has presented supply chain-dependent companies with both lucrative opportunities and considerable threat.

To repeat an earlier cited statistic, the World Economic Forum estimates that digitalization of the global marketplace will unlock $1.5 trillion in new business opportunities for logistics providers by 2025. Simultaneously, the logistics news cycle is filled with examples of businesses, small and large, whose operations were turned upside down by cybercriminal activity — sometimes with disastrous and long-term repercussions.

The thin line between these opposing futures boils down to smart choices. Decisions not just about the technology in which a company invests, but also what kinds of corporate partnerships it chooses, its management and human resource decisions, and ultimately, who the company chooses to trust.

In the midst of these tricky challenges lies one crucial decision: who to turn to for third-party logistics support. IL2000 is an expertise-driven company whose vision is built on the belief that we should treat our client's profitability and security as we do our own. We understand the deep importance of trust, and we work hard to earn, maintain and grow that trust with rock-solid secure TMS software and industry-leading supply chain expertise.

Talk to us if you're seeking a safer way to manage your supply chain.

References

2022 State of the Third-Party Logistics Industry Report. White Paper, 3PL Central, 2022, https://www.3plcentral.com/2022-state-of-the-third-party-logistics-industry-report.

6 Best Practices for Supply Chain Cybersecurity. 2019, https://www.thomasnet.com/insights/best-practices-for-supply-chain-cybersecurity/.

8-K - MARTEN TRANSPORT LTD (0000799167). SEC Submission, Securities and Exchange Commission, Oct. 2021, https://sec.report/Document/0001437749-21-024381/.

Best Practices in Cyber Supply Chain Risk Management. National Institute of Standards and Technology, 2020, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

Bhat, Manjunath, et al. How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks. White Paper, Gartner, July 2021, https://www.gartner.com/en/documents/4003625.

Cafferky, Brandon. "6 Lessons Learned about Cybersecurity and Freight in 2021." FreightWaves, 2 Jan. 2022, https://www.freightwaves.com/news/6-lessons-learned-about-cybersecurity-and-freight-in-2021.

Cost of a Data Breach Report 2021. IBM, 2021, https://www.ibm.com/security/data-breach.

Cybersecurity for Transport and Logistics Industry. White Paper, Infosys, Jan. 2020, https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf.

"Far More Companies Are Buying Cybersecurity Insurance." Investopedia, https://www.investopedia.com/cyber-insurance-increasingly-a-necessity-for-businesses-5086947. Accessed 29 June 2022.

Framework for Improving Critical Infrastructure Cybersecurity. Framework, 1.1, National Institute of Standards and Technology, Apr. 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Hawes, Clarissa. "Breaking: Marten Transport Falls Victim to Possible Cyberattack." FreightWaves, 4 Oct. 2021, https://www.freightwaves.com/news/breaking-marten-transport-falls-victim-to-possible-cyberattack.

Khoshniyati, Amir. Integrating NFC and Blockchain - Inbound Logistics. June 2022, https://www.inboundlogistics.com/cms/article/integrating-nfc-and-blockchain/.

Olyaei, Sam, and Claude Mandy. Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem. White Paper, Gartner, Jan. 2022, https://www.gartner.com/en/doc/757928-predicts-2022-cybersecurity-leaders-are-losing-control-in-a-distributed-ecosystem.

"Phishing Scams." Federal Trade Commission, 31 Oct. 2018, http://www.ftc.gov/news-events/topics/identity-theft/phishing-scams.

Protecting Air, Rail, and Maritime Control Systems With the Fortinet Security Fabric. White Paper, Fortinet, 2022, https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-fortinet-transportation-and-logistics-cybersecurity-solution.pdf.

QuizzClub.Com — The World's Largest Collection of Quizzes, Trivia Questions, Personality Tests, 3 July 2018, https://quizzclub.com/trivia/approximately-how-many-copies-of-war-and-peace-can-be-comfortably-saved-on-an-8-gb-gigabyte-flash-drive/answer/1427750/.

Resilience 2022. White Paper, Interos, Jan. 2022, https://www.interos.ai/resilience-2022/.

RiskRecon. State of Third-Party Risk Management Report | RiskRecon. https://www.riskrecon.com/state-of-third-party-risk-management-report. Accessed 28 June 2022.

S, Barrett. "How Much Data Is Produced Every Day in 2022." The Tech Trend, 30 May 2021, https://the-tech-trend.com/reviews/how-much-data-is-produced-every-day/.

Sobers, Rob. Data Breach Response Times: Trends and Tips. June 2020, https://www.varonis.com/blog/data-breach-response-times.

Strengthening the Detection of Software Supply Chain Attacks. White Paper, Esentire, https://www.esentire.com/resources/library/strengthening-the-detection-of-software-supply-chain-attacks.

References

Sundaresan, Bindu. "Best Practices to Protect Supply Chains - Inbound Logistics." Inbound Logistics, Oct. 2021, https://www.inboundlogistics.com/cms/article/best-practices-to-protect-supply-chains/.

Tabak, Nate. "Inside a Ransomware Attack on a Small Trucking Company." FreightWaves, 23 Feb. 2021, https://www.freightwaves.com/news/inside-a-ransomware-attack-on-a-small-trucking-company.

Tabak, Nate. "Ransomware Attack Hits Canadian Trucking Company Manitoulin." FreightWaves, 14 Sept. 2020, https://www.freightwaves.com/news/canada-trucking-company-manitoulin-hit-by-ransomware-attack.

Tabak, Nate. "US Recovers $2.3M of Ransom Paid to Colonial Pipeline Hackers." FreightWaves, 7 June 2021, https://www.freightwaves.com/news/us-recovers-ransom-paid-to-colonial-pipeline-hackers.

Tabak, Nate. "Why a Trucking Company Called a Lawyer Minutes after a Ransomware Attack." FreightWaves, 1 July 2021, https://www.freightwaves.com/news/why-a-trucking-company-called-a-lawyer-minutes-after-a-ransomware-attack.

Targett, Ed. Ransomware Attack Cost Expeditors $60m in Remediation, Lost Business, The Stack, May 2022, https://thestack.technology/expeditors-ransomware-costs-freight-forwarding/.