accenture

SECURING THE SUPPLY CHAIN

Understanding and mitigating the security risks of modern enterprise supply networks

You're only as secure as the weakest link in your supply chain

Supply chain security is a real and growing issue for modern enterprises.

As traditional linear supply chains are transformed into more flexible, digital and connected customer-centered networks, the number of external links an organization has with others (and the volume and sources of data that flow through those connections) grows exponentially.

But so too does the number of potential risks and vulnerabilities. This applies to both physical and cyber supply chain security. Larger, more flexible supply chain networks provide malicious and criminal actors with a bigger cyber-attack surface to target. But they also create more points of potential vulnerability in the flow of physical products and components through the value chain. The organization has to work that much harder to ensure the physical and digital security of its products and services.

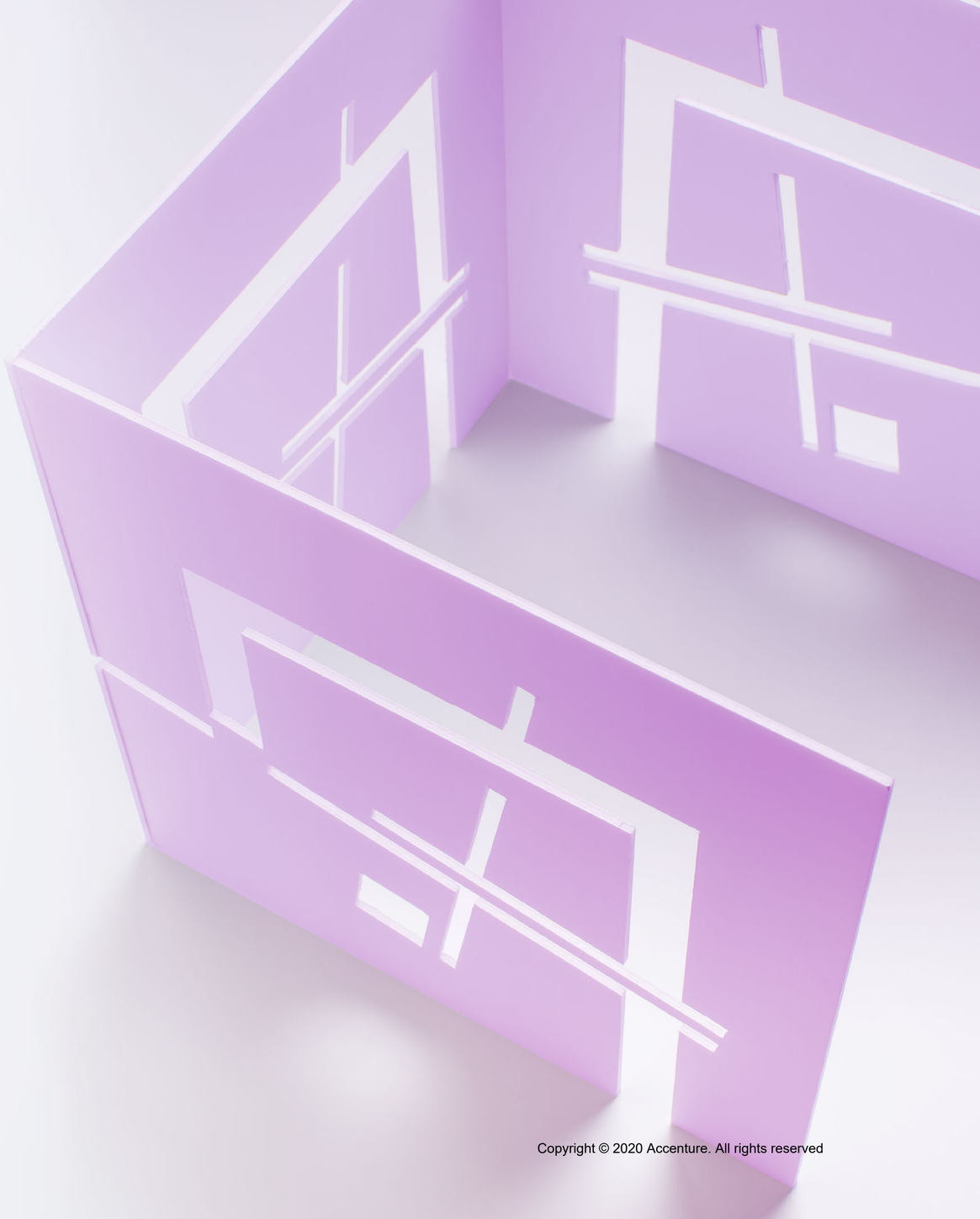
The COVID-19 pandemic is pushing these trends into overdrive. Organizations are doubling down on digitization to increase their agility and responsiveness and be better prepared to deal with the impacts of the pandemic and its aftermath. As they accelerate their creation of cloud-based open architectures, with cognitive engines powering acute sense and response capabilities, enterprises are exposing themselves to an exponential increase in vulnerabilities. Additionally, some organizations are also reverting to alternative suppliers which have not been thoroughly vetting their cybersecurity posture, thus exposing them to new avenues of attack.

The **NotPetya** attack of June 2017 amply demonstrated the destructive and disruptive power of malware. Initially appearing to be a geopolitical attack aimed at paralyzing government and business operations in Ukraine, NotPetya spread rapidly.

In fact, within a matter of hours, the malware had infected countless machines around the world, irreversibly encrypting master boot records, and crippling numerous multinational corporations in the process (including shipping giant Maersk, global pharma Merck, and food producer Mondelēz).[1]

Supply chain complexity in the New

In recent years, to meet customer and market expectations, supply chains have been reconfigured for agility, transparency and speed.



That's happened because consumers want new and better products faster than ever. They also demand unprecedented real-time visibility into supply chains, whether that's because they want to validate a product's authenticity or sustainability credentials, or simply understand exactly when it will be delivered.

To meet these elevated needs, enterprises have expanded their supply chains, made them more flexible, and integrated their suppliers more closely. In many cases, they've allowed suppliers to plug directly into enterprise systems to speed up data sharing. And of course, each of those suppliers may have its own equally integrated and complex supply chain to manage as well.

The result: enterprise supply chain networks have many more nodes—and many more potential points of failure—to consider. And the cybersecurity attack surface now extends far beyond the four walls of the enterprise.

Any weaknesses in supplier systems become weaknesses in enterprise systems.

AVIVORE is a sophisticated nation state adversary responsible for a series of linked intrusions against multinational organizations in aerospace, defense, and related industries (including automotive, consulting, engineering, civil nuclear and space and satellites).

Despite the target companies having significant cybersecurity capabilities, AVIVORE was able to steal data by gaining access through smaller high-tech engineering businesses that sat within those companies' supply chains (including by hijacking web browser information and related authentication information).[2]

The greater the complexity, the greater the risks

Consider the range of different nodes within modern supply networks. It's about much more than simply manufacturing plants, warehouses and transportation.

You now also have numerous third-party relationships, including cloud providers, facilities vendors, benefits providers, IT service providers, legal counsel, office suppliers, and many more. And each of these is now more likely than not to have digital as well as physical connections.

These networks are far more complex than the linear supply chains that preceded them. And, as each new node is connected or as each individual supplier is given access to core systems, the security risks and vulnerabilities increase. In fact, as these networks become almost boundaryless, traditional "four walls" security is becoming near impossible to enforce. Consider that more than 40% of cyberattacks are now thought to originate in entities within the extended supply chain or by external parties exploiting security vulnerabilities within that supply chain.[3]

COVID-19 is adding to the challenge. Businesses are managing unpredictable workforce availability, restricted supply routes, supply shocks, and highly volatile demand for some products.

They're having to react quickly to shore up supply chains, explore alternative suppliers and expand the use of digital collaboration technologies. Changes that might have taken years to implement are being compressed into a matter of weeks: just look at the huge and sudden worldwide uptake of video meeting solutions like Zoom. This rapid diversification and digitalization of supply chains is a necessary response to the pandemic. But it also massively increases the security risk.

Supply chain traceability can be a critical capability for enterprises looking to secure supply chain networks which have vastly increased connectivity and flexibility – and thus have many new points of potential vulnerability. An end-to-end traceability capability can massively help enhance the organization's ability to identify the position and provenance of individual units within the supply chain. That could bring all kinds of benefits to manufacturers, ranging from better regulatory compliance, to improved anti-counterfeiting, to near-real-time inventory tracking and management, to support for new consumer-facing provenance and authenticity solutions.

Understanding the global cyber-threat

Just as modern supply chains are global, so are the threats, particularly when it comes to cybersecurity. Threat actors are not bound by geography and can target any point in the supply chain.

Five key factors

Accenture Cyber Threat Intelligence's 2019 Report identifies the five key factors that are influencing this dynamic security landscape:

#1

Compromising geopolitics.
Cyberthreat actors are taking advantage of geopolitical crises to launch phishing lures, malware targeting, and disinformation campaigns. The global disruption caused by COVID-19 will present significant openings for these activities, but it is just one (albeit extreme) example of many such opportunities that already exist.

#2

Cybercriminals adapt, hustle, and diversify.
Conventional cybercrime and financially motivated attacks will continue to pose a significant threat. But criminal networks are growing in maturity and resilience. Threat groups are finding weak points, bypassing network defenses and then selling this access to other threat groups. This same access can be sold multiple times to multiple adversaries. They're also shifting their tactics to reduce the risk of detection, working in close-knit syndicates, increasing the precision of targeting, and taking advantage of their familiarity with local environments.

#3

Expanding motives for ransomware.
The rationale for ransomware attacks on corporations is increasingly more than just financial. Ideological and political factors are also in play. Organizations must maintain their abilities to prepare, prevent, detect, and contain these attacks, accepting that, if the motives are not financial, ransom payments may not rectify the situation.

#4

Improved ecosystem hygiene is pushing threats up the supply chain.

As enterprises improve their own security, malicious actors are turning their attention to their suppliers. Organizations must look to expand their visibility over this increased threat profile, integrating cyberthreat intelligence into mergers & acquisitions and incorporating vendor and factory testing into their processes.

Conducting security testing of products and services from supply chain should be prioritized based on risk analysis from cyber threat intelligence and correlation with internal vulnerability analysis.

#5

Vulnerabilities in cloud infrastructure demand costly solutions.

The multiple side-channel vulnerabilities recently discovered in modern CPUs are a significant risk for organizations running their compute infrastructure in the public cloud. Adversaries can use these vulnerabilities to read sensitive data from other hosts on the same physical server. Mitigations are available, but most come at a cost of reduced performance.

LockerGoga is a ransomware variant that hit numerous companies in the engineering, chemicals, and metals industries, possibly by opportunistically exploiting RDP systems with weak or already-compromised credentials to serve as access points for a site-wide ransomware campaign. Interestingly, the true goals of LockerGoga may have been destructive rather than financial. Later versions of the malware made it difficult to log back into infected systems, meaning victims struggled to actually pay the ransom demanded.[4]

The solution? Make security a core part of the intelligent supply chain

To manage these growing threats, organizations need to embed security principles all the way across the supply chain network. That includes making cybersecurity a priority not just within the enterprise, but also with all connected partner organizations.

It also includes developing traceability solutions for improved visibility across the network. These should be central considerations in the design of any intelligent supply chain.

The result will be a more secure enterprise and more secure supply chain. But consider also the potential for brand perception if a business can provide assurance to its customers about the security of products across its entire supply network. Or consider the negative perception if it can't.

This is likely to be an increasingly salient factor in purchasing decisions as awareness of the security risks increases.

No industry is exempt. While obvious target candidates are likely to be product-focused (such as consumer goods, pharmaceuticals and industrial products), other sectors also face considerably increased risks. Take automotive, for example. Connected vehicles could become lethal weapons if successfully hacked and misdirected. The implications for sectors like aerospace and defense are equally grave.

Or what about the regulatory implications? For sectors like telecommunications, critical infrastructure, aerospace, and defense, ensuring supply chain security and transparency is becoming an existential question. Regulatory requirements like the Cybersecurity Maturity Model Certification (CMMC) and NIST SP 800-171 are put in place to combat the growing cyber threats across the supply chain, making cybersecurity a foundational requirement for government acquisition of commercial products and services.[5]

This kind of certification may well be extended to other sectors (such as financial services) either as direct legal requirements or de facto standards as businesses look for systematic ways to validate their suppliers.

Accenture is helping a **global food company** improve its supply chain transparency—and build more trust with consumers in the process. With a central database collecting and checking valid product serial numbers, a blockchain platform integrating logistics events on the downstream supply chain, plus unique QR codes printed on packaging, the company is able to offer customers a new level of assurance about product authenticity. They simply have to scan the code and get access to a dedicated website where they can check authenticity and get some insights into a product's route through the supply chain. This website can also act as a means of alerting customers in the case of product quality issues.

Five practical steps to get started

Here are some practical recommendations for embedding security across the supply chain:

STEP
01

Create a "center of gravity" with a dedicated program office.

A key challenge for many enterprises is the complex, multifaceted, often fragmented nature of supply chain security. It can feel too big, too unwieldy, too overwhelming for any one part of the organization to get a handle on properly. By creating a single coordinating program office for supply chain security, organizations can help overcome these difficulties. This may include the need for a dedicated supply chain security risk officer.

STEP
02

Get visibility into the whole supply chain.

Look to improve the organization's visibility of all nodes in the supply chain, including their security posture. The program office should be the place to do this, creating a central team able to coordinate all the interested enterprise functions (supply chain management, IT, human capital, legal, etc.) and bring together all relevant data (including from external parties) for a more comprehensive analysis.

STEP
03

Understand the threats and weaknesses holistically.

Effective supply chain security must be holistic in nature. Moreover, to address risks, they first have to be identified. By centralizing the data and analysis in the program office, the enterprise is better able to put all the pieces together and see threats developing that were previously hidden in fragmented data. It can also help identify security gaps, weak points and vulnerabilities far more effectively.

STEP
04

Create a toolbox of solutions – and use it.

Build a toolbox of security solutions to cover potential supply chain vulnerabilities. For most enterprises, this should comprise some combination of asset management, security monitoring, legal contract review and management, vendor/supplier security posture assessment, and authentication for system access. Remember these tools are only effective if they are applied with the right approach, data correlation, and target product and services—for example, conducting hardware security testing on specific components from high risk suppliers or products prior to deployment based on risk score from cyber threat analysis and intelligence.

STEP
05

Maintain and monitor.

Resist the temptation to think that reaching a level of compliance and security means the hard work is done. Enterprises must establish the capabilities and commit the resources needed to sustain that security posture over time, remembering that both the threats and the organization's attack surface are constantly evolving. The effect of new M&A, new operating models and other changes – within the enterprise itself and within suppliers – must be continuously analyzed and accounted for.

FIN7 is a highly organized cybercriminal group specializing in targeted attacks against organizations in **retail, hospitality and financial services**. The group, which operates under the front of a legitimate penetration testing company, typically conducts spear-phishing attacks using malicious document attachments against selected individuals in targeted organizations. The malware delivered in these attacks has included the Carbanak implant and bespoke script-based implants such as HALFBAKED, Bateleur and DNSMessenger. FIN7 has also used a wide range of penetration testing tools such as Meterpreter, Cobalt Strike and Mimikatz for initial access and post-exploitation activities. [6]

Time to think holistically about supply chain security

Historically, supply chain security considerations have not been at the top of the C-suite agenda. That needs to change.

In today's hyper-connected world, and especially given the increased fluidity needed to manage the COVID-19 pandemic, the number of points of security vulnerability for connected enterprises are increasing exponentially.

An enterprise is only as secure as the weakest point in its supply chain network. Accordingly, leaders must now look to expand their security strategies and processes, working with their suppliers to increase visibility, understanding the threats and potential applicability and impact to their organization and supply chain holistically, and develop a range of flexible tools and best practices to mitigate the risks

Black Ghost Knifefish (also known as Dragonfly) is thought to be a state-sponsored threat group which has previously conducted supply chain compromises. The group gained significant notoriety in 2017 by targeting organizations operating in energy and manufacturing verticals based in North America and Western Europe. Its actors successfully compromised software produced by three ICS equipment providers located in Central and Western Europe.[7]

About the authors

Erik Olson
Managing Director,
Strategy & Consulting,
Supply Chain & Operations,
North America Lead

Royal Hu
Managing Director,
Accenture Security,
Supply Chain Security Lead,
North America

Lilian Ngobi
Functional Strategy Manager,
Accenture Strategy,
Supply Chain & Operations,
North America

Notes & References

1. Greenberg, Andy, August 22, 2018, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
2. Context Information Security, *AVIVORE – An overview of tools, techniques and procedures*, 22 October 2019, https://www.contextis.com/media/downloads/AVIVORE_An_overview.pdf
3. Accenture Strategy, *Chief Supply Chain Officers: Do you know where your weakest link is?*
4. Biasini, Nick, March 20, 2019, *Ransomware or Wiper? LockerGoga Straddles the Line*, Talos, https://blog.talosintelligence.com/2019/03/lockergoga.html
5. https://www.cmmcab.org, https://www.acq.osd.mil/cmmc and https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
6. Accenture Security, 2019 Cyber Threatscape Report
7. Accenture Security, 2019 Cyber Threatscape Report

About Accenture

Accenture is a leading global professional services company that provides a broad range of services at scale with strategy, digital, technology, and security services at our core. Accenture's Security Services Practice has been serving and partnering with clients for more than 20 years. We have successfully delivered some of the world's largest and most complex security solutions across multiple industries. Providing cybersecurity services is a standard part of what we do to help clients, to identify potential threats or critical issues requiring immediate response and areas for improvement and actionable recommendations to achieve desired outcomes.

Accenture has more than 7,000 security professionals spanning 67 countries, where we deliver cybersecurity services at speed, scale, and on demand that are aligned specifically to each of our clients' industries and unique business goals. Our cybersecurity consulting and delivery capabilities consist of highly trained security professionals, proven methodologies, cutting edge Research and Development (R&D) centers and partnerships with market leading technology vendors.

Visit us at accenture.com/us-en/services/security-index

About Accenture Research

Accenture Research shapes trends and creates data driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thoughtprovoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients.

Visit accenture.com/research