

Ebook

W / T H[®]
secure

Supply chain security: How to avoid the butterfly effect – and what it really means



This WithSecure™ special report explains how organizations must rethink supply chain cyber security to avoid the ‘butterfly effect’: small mistakes or oversights having much larger and more serious consequences later on. For the C-Suite, the lessons are numerous and sometimes unexpected, as business and IT leaders from different industries explain.

For this report, WithSecure™ spoke to security leaders in a range of digital, physical, and hybrid businesses, together with security experts and consultants. Some are quoted and others not, but all their viewpoints inform this document’s contents. External interviewees appear under Chatham House rules.

Contents

Introduction – The state of play
for digital supply chain risk 4

Technology challenges 5

Mapping the organization 7

Digital transformation: Simplify
or complicate? 10

What the butterfly effect really means 11

Security parallels 13

The real world of supply
chain attacks 14

Case Studies and Professional
Guidance 17

Conclusions 30

Introduction

The state of play for digital supply chain risk

In the 21st Century, few business terms are as misleading as ‘the supply chain’.

A chain is a series of linked, often identical things in a single line or loop. And while it may be comforting to think of supply chains in the old-fashioned sense – raw materials in, finished products out, containers on ships and boxes on trucks – today’s supply chains are almost never so linear, uniform, or analogue.

In a networked, information-based, omnichannel digital economy, even traditional supply chains rarely have a simple beginning, middle, and end, now that so many supporting processes and relationships have been digitized.

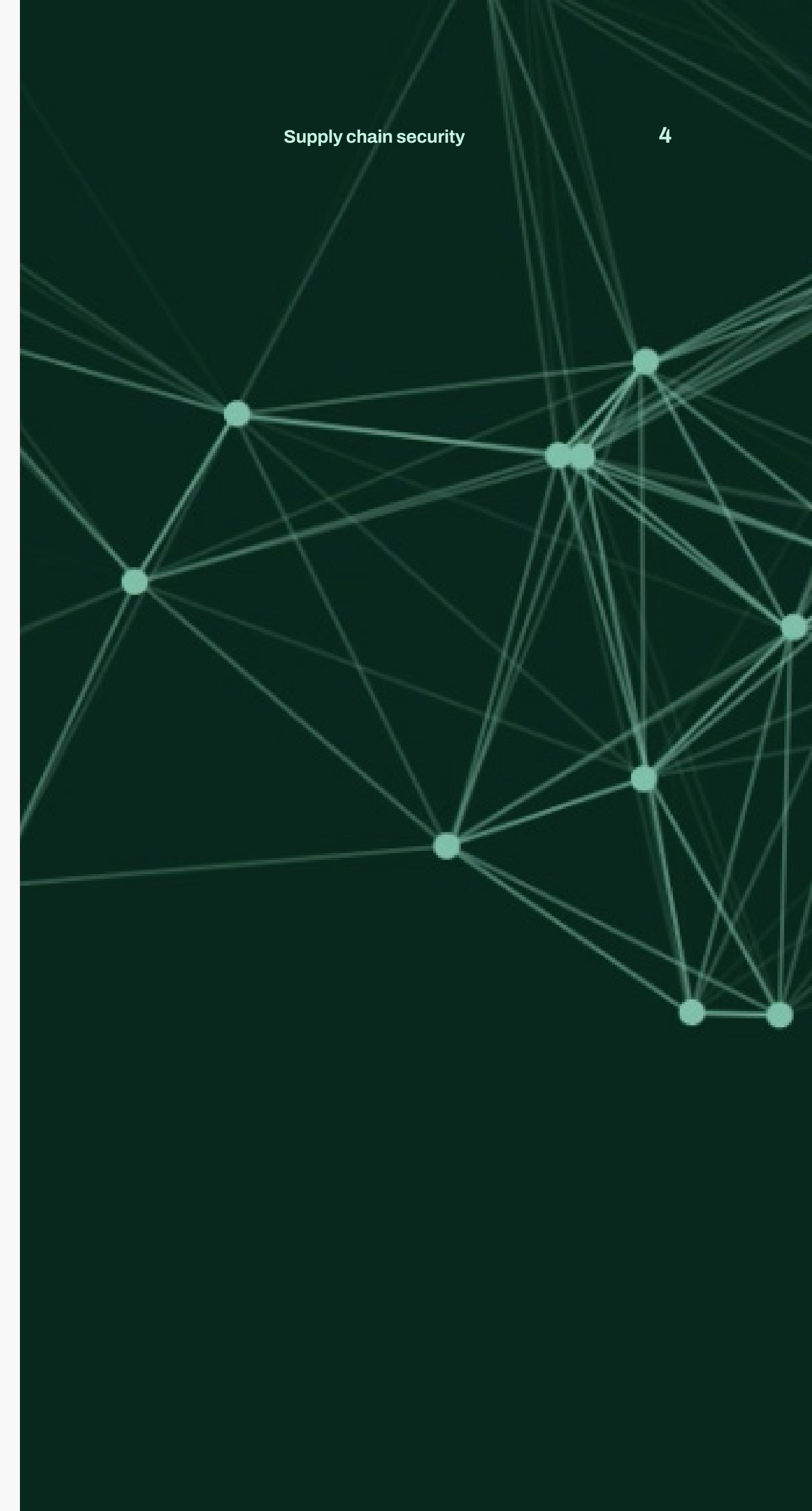
Supply chains are no longer a single line of dominoes on a table, perhaps, but more akin to a warehouse full of thousands arranged in interconnected patterns. Knock one piece over and we all know what happens next.

Domino dancing

But that metaphor no longer works so well for the modern supply chain, because dominoes are all the same size and shape. Any organization today might work simultaneously with the largest multinational or global technology platform and the smallest local start-up or app developer. In between will be businesses of every size and shape, supplying every type of good, material, or service – both upstream and downstream.

This is one reason why cyber attackers – organized criminals, hostile states, black-hat collectives, activist groups, or opportunistic hackers – are increasingly targeting our sprawling supply networks and ecosystems. Those supply chains can extend and amplify a successful attack’s impact and influence, spreading risk throughout entire industries.

For criminals, that’s good for business.



Technology challenges

DevOps risks

IT and DevOps teams often use open-source and other code repositories, reusing trusted components that have been coded by a global network of peers. Those repositories are themselves now under attack, as are popular cloud platforms, managed services, and utility applications.

According to WithSecure™ research, attacks on specific applications peaked in 2017, while hits on utility software hit apex in the following year. However, attacks on popular code repositories have been soaring since 2020 and are increasing every year. We should regard all these incidents as explicit assaults on trusted relationships and collaboration.

Two-way trust in software supply

So, when it comes to the software elements of your digital supply chain, WithSecure™ urges you to always select suppliers who are vigilant in cyber security – especially when providers may be small companies or sole traders.

Ask questions like:

- What do their permissions and policies look like?
- How much of your organization's personally identifiable information (PII) and intellectual property (IP) do they expose?
- Is cybersecurity a verifiable selling point for them?
- Do they employ their own security teams and consultants?
- And do they offer bug-bounty programs, rewarding white-hat hackers for finding new vulnerabilities and exploits?

But remember, in today's interconnected supply networks, your organization may ship or deploy a suppliers' code in your own products too, passing on any flaws to your users and customers.

So, ask the following questions of your own enterprise:

- Do you know what open-source components you are shipping in your products?
- Are you certain that externally sourced code is secure before using it?
- Is patching vulnerabilities a priority for you?
- Does your threat-modelling process extend to you as a supplier?

In short, to what extent might you be part of the security problem?

Catching the butterfly effect

So, there are better descriptors of the threat landscape today than the tumbling dominoes mentioned in our introduction. WithSecure™ believes that the so-called ‘butterfly effect’ is closest to the everyday reality of business in the 21st Century, a world in which we are all inter-related and interdependent.

Most of us have a simplistic idea of what the butterfly effect means: small actions (or inactions) having much bigger consequences over time. But later in this report we will uncover the concept’s deeper truths and its wider lessons for securing the supply chain.

But before then, where are we now?



Mapping the organization

The first thing to understand is that the IT perimeter of any member of a supply network now extends far beyond your head office – via cloud platforms, shared services, mobility, remote working, and more. This process accelerated during the pandemic and has made endpoint detection and defender systems essential to have.

This is why some security professionals now claim that the perimeter is dead. It isn't, but it has become much harder to map and quantify. Yet quantify it you must, to stand any chance of getting to grips with both external and internal cyber threats. How can you secure what you don't know you have – or spot attacks as they happen?

IBM X-Force Threat Intelligence Index 2021 revealed that scanning for vulnerabilities has overtaken phishing as the most common attack vector for cybercriminals – a process that may be automated. This both explains the soaring attack volumes on open-source and other code repositories, and increases the pressure on organizations to understand the assets at their perimeter.

The good news is that External Attack Surface Management (EASM) is fast emerging as a discipline for mapping and managing the perimeter before any weaknesses can be exploited. WithSecure™ has published dedicated advice on this subject, and we suggest you look at deploying EASM systems.

“What something like EDR [endpoint detection and response] does is shine a flashlight on potential vectors of attack. It allows you to, as quickly as possible, detect and respond to a supply chain attack. EDR can be the difference between sinking and swimming in an incident scenario because it buys you the time to catch up.”

Jordan LaRose, Director of Consulting & Incident Response, WithSecure™

Insecure people

Meanwhile, every employee will have their own networks of connections. At any of those touchpoints that employee could be compromised, whether by malicious code in an email or by someone reading their mobile over their shoulder. The knock-on effects of that could impact the whole organization – and far beyond. The classic butterfly effect.

Cybersecurity training and robust policies are important, but the potential for human error remains. Therefore you need an additional layer of security for endpoints, especially when employees are working remotely.

So, the key lesson is that supply-chain security is no longer a simple end-to-end process, but rather a complex mix of accumulated risks, interconnections, and interdependencies – including personal responsibility.

Let's explore what some of those are.

We are all downstream

In the old linear supply chain model, our suppliers were upstream from us and our customers downstream.

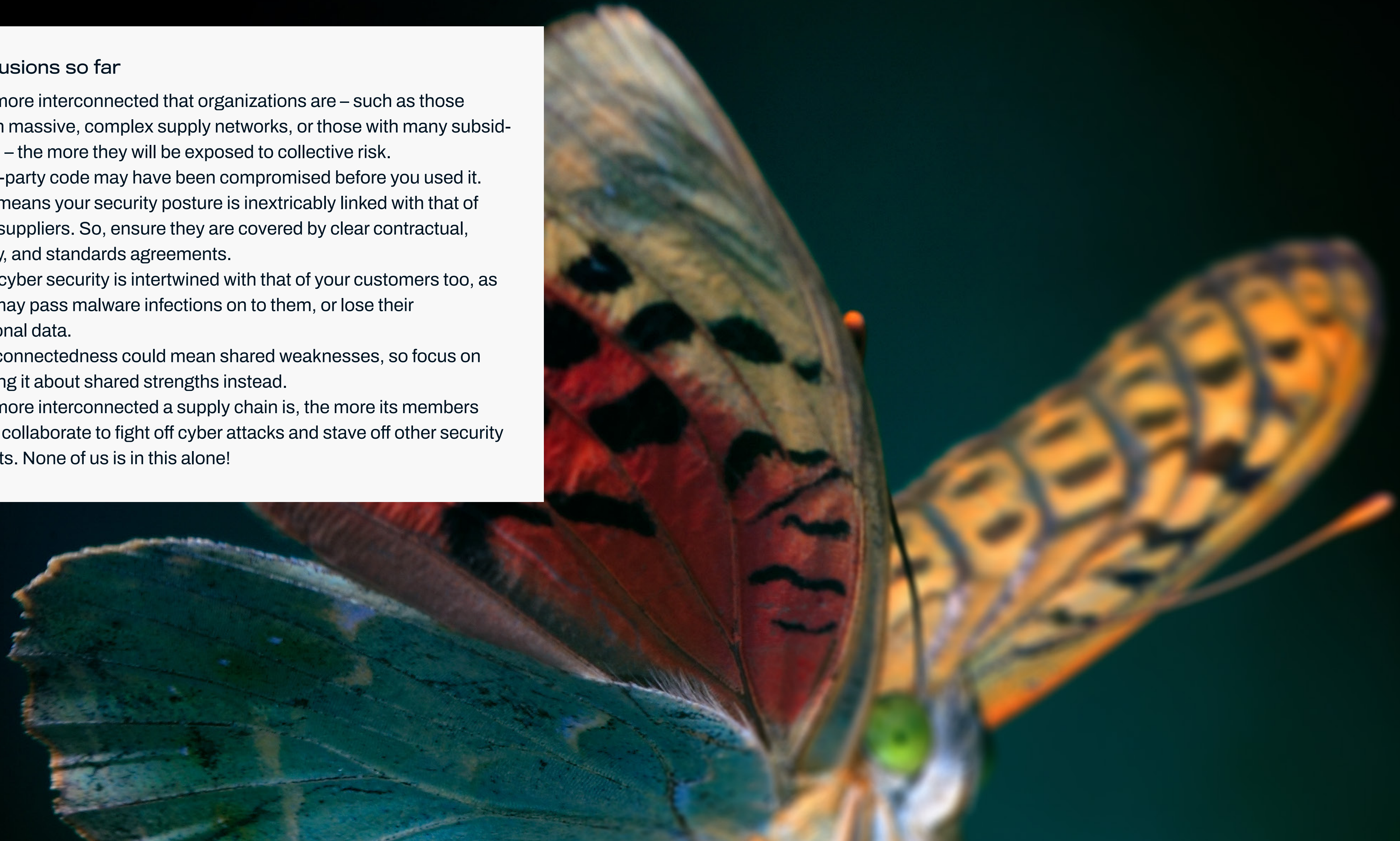
Those customers now interact with us in a multichannel world and trust us to keep their data safe, yet they could easily become collateral damage in an upstream attack. But equally, an attack on a customer – a company that buys our products or services, for example – could have complex repercussions for us higher up the chain.

So, in terms of cyber security today, we are all effectively downstream from each other in our modern supply networks, because a security breach might come from any part of that ecosystem and spread in any direction, with repercussions that become more serious as the risk is passed on.

Again, that's the butterfly effect

Conclusions so far

- The more interconnected that organizations are – such as those within massive, complex supply networks, or those with many subsidiaries – the more they will be exposed to collective risk.
- Third-party code may have been compromised before you used it.
- This means your security posture is inextricably linked with that of your suppliers. So, ensure they are covered by clear contractual, policy, and standards agreements.
- Your cyber security is intertwined with that of your customers too, as you may pass malware infections on to them, or lose their personal data.
- Interconnectedness could mean shared weaknesses, so focus on making it about shared strengths instead.
- The more interconnected a supply chain is, the more its members must collaborate to fight off cyber attacks and stave off other security threats. None of us is in this alone!



Digital transformation: Simplify or complicate?

At this point, contracts, SLAs, and KPIs become critical, but so do decisions about whether to standardize your IT infrastructure on a specific technology platform. Doing so will reduce complexity, but could make any successful attack on your supply chain more serious.

In this sense, digital transformation programs may have hidden impacts on supply chain security, given that their core purpose is often consolidation and simplification in the cloud.

The alternative is to go with a mix of best-of-breed systems. The security bonus here is that these are harder to target at scale, but they may also create an estate that is much tougher to quantify.

“Introducing complexity doesn't always equate to more risk. It may be that diversifying workloads helps you keep a critical service up and running.”

Jordan LaRose, Director of Consulting & Incident Response, WithSecure™

In general, however, such decisions are not ours to make in the supply chain, unless we are a multinational superpower or global tech platform, which may have the reach and clout to enforce their own standards and tell others how to operate. But with such great power may come too much ability to limit partners' opportunities to innovate.

“When you globalize things but the primary key for doing so is enforcing a set of standards, or reducing your costs, on the security side you are actually making things more vulnerable. It's much harder for an attacker to take out an organization if that organization is in 1,000 different bits. But when you bring it into one platform, they've only got one target to hit.

“So, in a transformation, you need to have areas of the business that are ringfenced off. But with digital transformations, it's often all about the transformation itself, or the money. Security is not in the same aisle. Your transformation people tend to come in, do a transformation, then leave the security problem for someone else.”

Jordan LaRose, Director of Consulting & Incident Response, WithSecure™

What the butterfly effect really means

All of this makes avoiding the butterfly effect a critical business priority. But what does this really mean? And what are its lessons for security leaders today? The answers are not all as obvious as you might think. To find out why, we should return to the source.

Although he didn't coin the term – that came later – American author Ray Bradbury's 1952 short story, *A Sound of Thunder*, introduced the concept of the butterfly effect.

In his cautionary tale, one of a group of time travelers to the prehistoric past strays off the safe path that his team must follow through a dangerous forest full of dinosaurs, and accidentally treads on a butterfly. Back in the present day, the team finds the world has been catastrophically changed, in countless different ways.

The first lesson is clear: one tiny mistake, even something apparently innocent, can ripple outwards with disastrous consequences. In the story, a single action echoes throughout history, with each knock-on effect being larger than the one before it – a feedback loop.

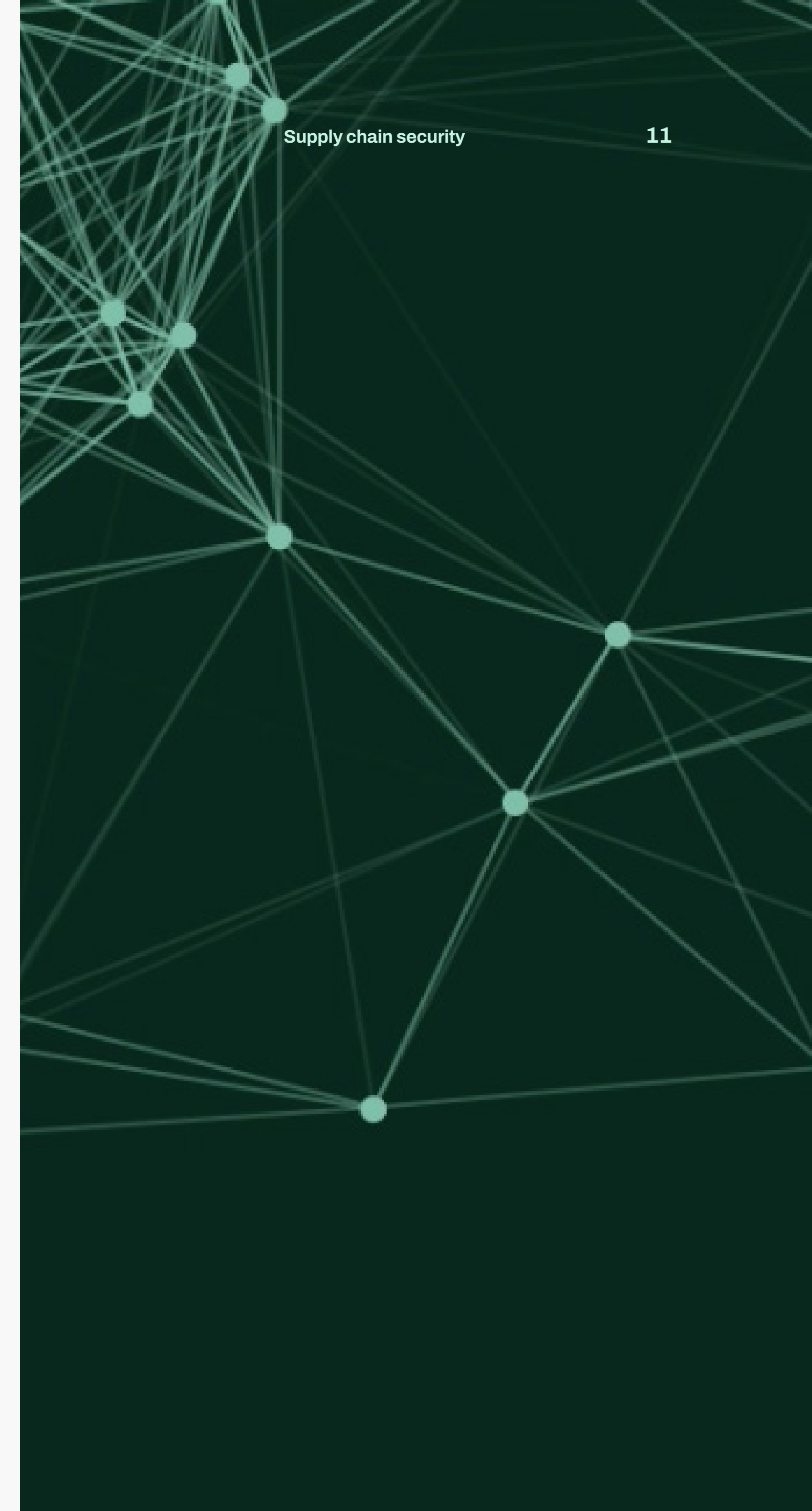
This idea of interdependencies in closed systems was proposed in 1800 when philosopher Johann Gotlieb Fichte noted that moving a single grain of sand would “change

something throughout all parts of the immeasurable whole”. Today we think in terms of technology ecosystems, a concept that underlines Fichte's point: small actions within them have holistic effects.

In the 1960s, meteorologist Edward Norton Lorenz popularized the concept by suggesting that a single flap of a seagull's wings could, over time, whip up a storm. Then in 1972, he changed the metaphor to a single beat of a butterfly's wings eventually creating a hurricane.

That powerful image stuck in people's minds, like an early meme. But Bradbury's original take is more instructive for organizations today, because in his story, the team learns other valuable lessons too.

So, what are those lessons?



Five lessons of the butterfly effect

1.

First, the team is unable to travel back to the point the mistake was made to undo the simple error. As a result, they have no choice but to live with its repercussions in a changed world.

That's like the lasting reputational, trust, and financial damage that may come from a data breach. We might have short attention spans today, but social networks give us unforgivingly long memories!

2.

Second, the butterfly effect was caused by an individual abandoning normal teamwork – if only for a brief, foolish moment.

That's like the staff member who forgets security protocols for a second and clicks on a tempting, apparently legitimate link that compromises the system for everyone. As we have seen, endpoint security would create an additional layer of protection in this scenario.

Today's complex supply networks demand much better and more responsible behavior: vigilance, plus constant teamwork and collaboration – especially with ransomware, crypto-jacking

(the remote use of others' computing resources to mine for cryptocurrency), and other malware attacks on the rise.

3.

Third, our time traveler ignored the cardinal rule that the whole team understood and signed up to before embarking on their shared venture: don't stray off the path. In the story, a safe path has been created that floats above the dangerous, primeval forest full of man-eating dinosaurs.

Again, an enforced security policy is everything, and organizations are only as secure as their weakest link. We are all individuals, but we are collaborating, working together as a team on the same path through a dense forest of shared risk and danger.

The 'monsters' may not be the real threat.

4.

Fourth, our hapless traveler was so worried about the tyrannosaurs that he didn't see the butterfly (and if he had, he might have been tempted to catch it, causing the same disastrous effects).

So, it wasn't the obvious monsters that posed real danger in the story, but instead something apparently harmless and easily overlooked. There may be millions of those fluttering about worldwide. (Never forget, the insects outlived the dinosaurs.)

5.

Lastly, in Bradbury's tale they find the butterfly on the sole of the traveler's shoe back at headquarters, in a world that no longer looks the same.

Perhaps one day in the past you trod where an attacker was hiding, then walked that threat into your head office when you accessed critical systems.

The message couldn't be clearer: Don't be that traveler!

“Some of the more sophisticated attacks in recent years have come from basic control weaknesses. Most successful attacks have been easy for the attacker to implement. People are doing lots of flash stuff, but not getting the basics right. You're making criminals' lives a hell of a lot easier if you haven't done the basics.”

EMEA Chief Information Risk Officer, multinational bank

Security parallels

The parallels with cyber security in today's complex supply-chain networks are clear.

We all know about organized criminals, hacker collectives, and hostile states – genuine threats, of course, and the equivalent of Bradbury's tyrannosaurs. And we have all heard of phishing, ransomware, trojans, viruses, malware, and data theft, all of which are lurking out there in the undergrowth of the internet's vast technology forest.

The challenge is that, in an increasingly cloud-based or hybrid IT environment, many hackers – including lone, have-a-go attackers – are now trying to make their attacks look like normal network traffic. Or as we have seen, they are attacking trusted tools and code libraries.

Detection in the cloud

Today's opportunistic cyber criminals increasingly look for ways to exploit normal functionality or poorly configured systems: to be the butterfly on the sole of your shoe at head office.

All of which makes threat detection a must-have for supply chain security, particularly in hybrid cloud estates. Such applications are moving away from the exclusively endpoint-based telemetry data of old, and towards what we might call the 'telemetry of actions'.

These are actions in the control plane of your cloud platforms – in the web of APIs that allows an administrator to create, modify, or destroy computing or data resources in a cloud environment.

Increasingly, sophisticated attackers use APIs like these to reach their goals. For example, they might create new user accounts, modify permissions on existing accounts, or grant access to resources from external locations. These activities create traffic that might appear legitimate to the unwary or inexperienced eye.

In other words, today's attackers might not roar and strike at your door – though they could do that too in a distributed denial of service (DDOS) attack or by hacking your corporate portal. Instead, they aim to flutter in through the window you've left half open.

Hundreds of millions of lines of malicious code are floating through the dense forest of our hybrid, interconnected infrastructures. Hostile forces want these to seem innocent and risk free. They want you to find them attractive, to allow them into the enterprise.

The real world of supply chain attacks

Fiction is all well and good, but are these attacks really happening, and in the way this report suggests? Emphatically, yes. There have been at least 200 dedicated supply-chain attack campaigns over the past decade – attacks that have each affected countless supplier networks and millions of customers. Plus, there have been numerous attacks on IT systems and applications that have impacted on supplier, buyer, and customer relationships, or damaged trust in institutions and brands.

Some of these attacks have been widely reported.

High-profile attacks: SolarWinds

In 2020, hackers compromised the Orion system made by US tech provider SolarWinds, adding malicious code to software that was trusted by 33,000 corporate and public-sector customers.

Unknown to SolarWinds, this infected code was sent out in standard software updates to at least 18,000 of those customers, making the vendor part of the attack vector in a rolling program that went undetected until 2021.

Throughout this period, attackers were able to use their exploits to access the internal systems of SolarWinds' customers – and the private data they held – to spy on them and install more malware.

Victims included the US federal government, one of the biggest and most secure supply chains in the world. In that process, some of America's security touchstones were hit, including the Pentagon, the Department of Homeland Security, and the National Nuclear Security Administration, not to mention several universities.

However, private-sector victims included IT behemoths Microsoft, Intel, and Cisco, compromising yet more trusted systems and supply chains, and striking at the heart of both the internet's core infrastructure and the enterprise cloud.

Exactly as in the story, a lone butterfly on a shoe changed the world.





High-profile attacks: Kaseya

The 2021 ransomware attack on software made by tech management provider Kaseya hit at least 1,500 different organizations. Russia-affiliated hacker collective REvil exploited two vulnerabilities to break into more than 50 managed services providers (MSPs), each of which sat at the center of complex supply-chain networks.

This was another attack that fanned out across others' digital supply chains, using customer trust to breach critical systems and, in the process, undermining that trust.

Other attacks have been harder to quantify, and therefore to combat, which is why vulnerability management is important in giving you a risk-based view of your whole attack surface.



High-profile attacks: Log4j

The late 2021 attack on free, open source, Apache logging utility Log4j allowed attackers to remotely execute code (an RCE attack).

Log4j is one of the most popular tools for recording and collecting data on users and online behavior, having been downloaded millions of times. In retrospect, therefore, it seems like an obvious target.

This is why thinking like an attacker is so important – even if specific threats are unknown. Ask yourself, what might an attacker use to compromise your systems? Carry out a red-team threat-detection exercise, modelling possible attack patterns. Or use a purple-team model, combining offensive and defensive (blue) tactics.

The Log4j attack has so far been linked to ransomware, cryptojacking, and numerous other incidents. But its longer-term repercussions remain unknown. It may have been the biggest supply chain attack to date; certainly, it was rated 10/10 for risk on MITRE.



High-profile attacks: NotPetya

However, the attack with the biggest financial impact to date was the 2017 NotPetya malware assault on Ukrainian tax-filing application, ME Doc.

Use of this software was mandatory for every tax-filing business in Ukraine: at that time, a total of over 400,000 enterprises. Spreading via updates and other methods, the attack cost organizations an estimated \$10 billion, mostly in collateral damage.

As more and more nations digitize fiscal dealings between citizens, businesses and government – the UK recently ordered some tax returns to be filed via dedicated software at the user's end – these types of attack will inevitably become widespread.

More, they exist in a world in which the public sector seems keen to make it the private sector's problem, pushing the security onus away from government and onto SMEs and sole traders. In the UK, 99 percent of companies are SMEs. Therefore, a successful attack on SMEs' tax affairs would be catastrophic: in other words, highly profitable for criminals.

“Some of the more sophisticated attacks in recent years have come from basic control weaknesses. Most successful attacks have been easy for the attacker to implement. People are doing lots of flash stuff, but not getting the basics right. You're making criminals' lives a hell of a lot easier if you haven't done the basics.”

EMEA Chief Information Risk Officer, multinational bank

Utility attacks

Other successful anti-supply-chain campaigns have included attacks against utility software, such as code-testing application Codecov. In that incident, scripts gathered user credentials and sent them to the attackers, giving them privileged access to Git repositories (virtual code hubs) for more than two months before the incursion was discovered.

This underlines the point that many of today's supply chain attacks don't roar and beat their chests like Bradbury's monsters, but steal credentials to mimic normal network traffic. In this way, they can pass unnoticed for long periods – yet another butterfly on the enterprise's shoe.

Cyber criminals generally target libraries that are used in larger products. Again, this emphasizes the need for red- and purple-team security exercises that model how attackers might sneak into your supply networks unobserved.

Hardware attacks

Though comparatively rare, there have been examples of attackers compromising the physical IT supply chain, too, implanting backdoors into hardware components.

For example, WithSecure™ knows of an upstream microchip company which discovered that a backdoor had been printed into the firmware of every graphics chip it had been releasing, until the backdoor was finally discovered and wiped from the library.

The chipmaker found that attackers had compromised a Web-based integrated development environment (IDE), through which they had been able to access a developer account, write the backdoor, and upload it to the central code repository.

The hidden cost of supply chain attacks

But while many of these anti-supply chain campaigns have had known, quantifiable effects, most have hit every organization to a lesser degree.

That's because of a little-considered consequence of major supply-chain incidents and breaches: every security team has to investigate whether their organization has been affected by the attack. Even if, in most cases, it transpires that they have not.

As such, supply-chain attacks are truly insidious: they have a global impact in terms of time, money, skills, and human resources, and this diverts organizations from focusing on their strategic business objectives.

That's one of the challenges reported by our first case study interviewee.



Case Studies and Professional Guidance

Case Study: The hybrid retailer: A modern supply chain

Our first case study is a major European retail group with some unusual elements: it is one of the big two diversified retailers in its home nation. Its network of physical and online stores sells a full range of goods, including food, to a country that has a relatively small population.

However, each store is an independent cooperative that hands its profits back to the customers who own it. Each outlet is free to act with autonomy, albeit within a popular, well-managed, overarching brand. The group also has a successful cooperative banking arm and fuel stations, and owns its logistics operation.

Yet it is also a modern, hybrid supply network, not just a traditional business selling goods to customers. The company acknowledges that it has over 800 IT suppliers, 150 of which provide critical services or tools. Vendors include most of the world's major public cloud platforms, alongside small local providers and independent developers.

Where integration begins... and ends

So, the group's wider supply chain is large and, in some respects, well integrated. But in others, it is essentially a loose affiliation of organizations and private companies of every size, which work together with shared aims.

Cooperation is therefore essential to making the whole system work. The fact that the customers also own each outlet – rather than an offshore investor or maverick billionaire – means the group has built-in incentives to remain secure for everyone's mutual benefit.

Despite this, the company reveals that some individual cooperatives go it alone on key decisions – including technology choices – simply because they can. Following the letter and the spirit of the rules is not always the same thing when it comes to supply chain security!

However, the Information Security Manager in the parent organization's Risk Management team explains:

“ We have always emphasized, especially in information security, that individual cooperatives cannot make risk decisions on any matters.”

The group's unusual mix and structure also mean that customer data theft is a relatively minor concern for the group. With a national population smaller than some capital cities, and the group's customer base being just under half of that, domestic hackers could obtain much the same information from anywhere in the country.

So, there would be little to gain from compromising one of the two critical organizations that supply so much to so few people – unless the attackers come from a hostile state, of course, and wish to destabilize the country.

Brute-force campaigns

The fact that DDoS attacks are this venture's most frequent supply chain incidents suggests that we can no longer discount hostile states as being the source of even low-skill, blunt-instrument attacks on popular consumer brands.

So, to what extent was this major retail group the victim of global attacks, such as SolarWinds, Kaseya, or Log4j? The Infosec Manager acknowledges that the group was hit – but not in an obvious way:

“ We were certainly affected, but only in the sense that we had to spend literally hundreds of hours investigating possible effects. Log4j, or Log4Shell, was a major concern. We spent a lot of time on investigations, emergency operations, and emergency meetings, though we never found any breaches.”

But he adds:

“ However, we made a lot of changes in response to those investigations, so it was not a waste of time. SolarWinds, again, was not a major issue for us, but we did spend a significant amount of time investigating it.”

Time spent, not time wasted

So, proactive investigation is an important, if often frustrating, supply-chain reality: hours spent checking for vulnerabilities that may not exist. But in the process, security teams shore up core systems and understand where threats could occur in the future.

What other lessons did the group learn from these critical exercises? He says:

“ These major vulnerabilities come along every three or four years, but what it goes back to is basic security controls.

“ If you have a proper vulnerability management system in place, and a proper CMDB [configuration management database, storing key information about your hardware and software estate], and if you have proper supply chain management, you have everything. So, when a vulnerability like Log4j comes along, it's so much easier to start investigating.”

In short, understand your perimeter and what is really within the walls of your extended estate. But sometimes this may clash with other business priorities, he warns:

“ When you talk to the leadership and tell them, ‘Our CMDB is not up to date, about 30 percent of that data is missing’, they will say, ‘We recognize it's an important issue, but right now we have other stuff for you to do’.

“ Then suddenly you have to investigate an issue like Log4j, which requires you to have all the data and to properly do the analysis. At that point, not having the data becomes a major problem.”



Case Study: The multinational media conglomerate

But what can you do if your company is an umbrella organization for literally thousands of trading entities, rather than dozens or hundreds? And when you are the core element in a broader supply-chain network that runs to tens of thousands of partners – over 130,000 by some estimates?

That's the challenge facing one media and communications behemoth. The Fortune 500 giant's Security and Assurance Manager admits to the huge scale of the cyber security problem facing the company – one that is akin to that forest of primeval dangers. Only this time the dangers may be within the enterprise itself:

“ In a normal organization, you would have a supplier risk-management function. Ideally, that function would know who, and where, all your suppliers are, and what products are being used. And you may have intel: threat-monitoring on key suppliers.

“ But none of that is possible in our environment, where we have thousands of companies, ranging from 20-30 employees to hundreds or thousands. We don't have a centralized and effective supply-chain function in the way that most traditional large organizations do.

“ So, a lot comes down to us setting the security policy, plus there's a compliance team. I'll set the standards on the compliance side, saying, 'These are the policies we expect individual companies to adhere to'. And in turn, they will have their own risk and supplier-management teams.”

Where the buck stops

However, even such a broad oversight function needs to be strictly managed and its policies rigorously enforced and policed. That's because while a subsidiary might be the attacker's initial target, the buck stops with the holding company in legal, regulatory, reputation, and investor terms.

So, has the Assurance team been able to make real-world security gains by thwarting attacks lower down the supply chain? Yes, he explains:

“ While one of our companies had done normal due diligence on suppliers, we spotted an instance when they were asking a start-up to undertake something dangerous: running a system that could have put the whole company at risk, had it not been managed and secured properly. My team stepped in and said, ‘No, this is unacceptable.’ ”

Digital don'ts

Digital transformation was at the heart of this issue, he explains:

“ Our constituent companies run their own instances of particular cloud platforms, but there was a project to bring several of these together within a single instance of one platform. But that consolidation meant creating a way to standardize configuration settings across 20 or so cloud instances. The start-up said they could do that. ”

“ However, the danger came to my attention when I saw service accounts appearing on that platform which had global admin rights, but they didn't have multifactor authentication enabled. That rang alarm bells straightaway. ”

“ So, it wasn't the start-up's core technology which was at fault; that could have done the job. I could see straight away that here was a tool with global admin rights to multiple instances of a major cloud platform. Had that been compromised in any way, the attacker would have had full control over all of the tenants. ”

There was an added dimension to this astute avoidance of threat, he explains:

“ Not only did I not have any confidence in a start-up with so few people in it being able to secure their system properly, but they also had no money in the bank. In other words, no money to pay any legal compensation that might arise from their mistake. So, the IT function having no clue about the supplier risk element is where we had to step in. ”



Other markets: The IoT challenge

Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices have been under sustained malware, crypto-jacking, and ransomware attack in recent years. In some cases, this has been in the form of surgical hits on soft targets, in sectors such as (appropriately enough) healthcare, plus national and local government.

One trigger for this is, despite the growth of Secure By Design initiatives, many smart, connected devices are still rushed to market with insufficient security controls in place. Meanwhile, users often neglect to change preset factory logins and passwords – credentials that may be known to attackers.

Insecure hubs, cameras, HVAC units, and even smart lightbulbs may offer attackers covert routes into an organization's systems and, from there, out into the wider supply network. A rich data harvest awaits the masterminds of any successful incursion.

The 'world in a box' problem

Remember, individual products may, in themselves, represent a complex network of supplier relationships. These might include the makers of hardware, firmware, operating systems, standalone applications, and electronic components.

Plus, there may be wider partner affiliations in place for data-gathering, marketing, research, and advertising. These may be invisible to the user, and perhaps even to other partners.

To give some indication of the IoT challenge when it comes to security, trust, and transparency, a 2020 Consumers Association report found that one popular smart TV model sent data about the viewer to 700 different IP addresses in just 15 minutes. The data regulation aspects of that alone are incendiary.

So, IT and data security managers should be clear about who owns the IoT in the organization. Plus, they should invest in technical talent, and never underestimate the change-management challenge in terms of governance, skills, organizational behavior, systems, and processes.



Other markets: Manufacturing

This cyber security challenge deepens when organizations are dealing with devices that were never designed to be exposed or connected to the internet in the first place.

Again, this applies to vulnerable sectors such as Healthcare – where medical appliances can’t easily be retrofitted, ripped out, or replaced – and Manufacturing, where ageing industrial control systems (ICS) pose similar difficulties.

In general, sectors like Industrial and Manufacturing also shift the security focus away from IT and towards operational technology (OT). In these instances, prioritizing cyber security from the get-go, starting at the hardware layer, is critical to developing end-to-end security practices.

Proactively change your IoT environment, building and controlling your estate with extreme care and due diligence. WithSecure™ security consultant Michael Weng explains:

“ One important aspect of my work is making our clients aware of IEC 62443 [an international standard for industrial and control systems].

“ A core part of that standard is a set of requirements that you, as asset owner, can put on vendors or integrators when you're building a facility and using their equipment. It's a way to voice which security requirements you need from a cyber security perspective, so you can avoid being a victim of supply-chain attacks.

“ But it is just one thing working with standards and compliance. It’s also about the software-development lifecycle, ensuring that the vendor incorporates secure development into it to reduce the number of possible supply-chain attacks.

“ You also need to have controls and policy frameworks in place to ensure your certificate of authorization, use, and distribution is secure, otherwise somebody could compromise it.”



Controlling the control systems

So, how should security and OT managers tackle the challenge of industrial systems that were not designed with the internet in mind – in smart factory initiatives, for example?

Weng explains:

“ We are still tangling with the legacy issues of devices that were never meant for the network or the internet and, as such, represent a clear and present danger.

“ Since they do not have modern, sufficient cybersecurity controls, they cannot protect themselves and so can’t protect our networks and other systems from them. In this way, they become a vector for adversaries to penetrate IoT and IT networks.

“ We need to close down those access points and reduce the attack surface. One way of doing this is via a ‘defense-in-depth on your layer’ technique. This is where you build additional layers of controls and countermeasures on top of those devices, putting as many obstacles as possible in the way of an adversary getting in.

“ But at times you just need to be realistic: you need to have segregation from the internet and segregation from business IT systems.”

Other markets: The Services sector

The Services sector is crucial to many economies. According to UK government figures, for example, Services account for roughly 81 percent of Britain’s gross domestic product (GDP) and 82 percent of jobs.

Services have become increasingly digital, a trend deepened by markets such as Financial Services becoming more app-centric for consumers and businesses alike – not just in banking, but also in payments, wealth management, investments, and more.

The pandemic accelerated the trend towards low-friction, mobile services, and away from in-person alternatives. This was spurred by a booming FinTech market in the US and UK, and by initiatives such as Open Banking.

Case Study: The multinational bank

A billion-dollar US multinational company in fields such as corporate banking, investment management, and asset servicing is an obvious target for cyber criminals, especially when its core customers are wealthy institutions and high-net-worth individuals.

However, the company's EMEA Chief Information Risk Officer says that being digital isn't the whole story of supply-chain security:

Security is about people

“ If you're in Financial Services, you're generally focused on technology and processes. But the people element plays an equally vital part in the security triangle.

“ One of the keys is communication. How can you impart important security information to a group that doesn't have much interest in the topic? Beyond ‘Are we okay? And if we are, then then let's move onto something else.’

“ If you only have 15 minutes to sell your security message, then concise communication – a story that gets to the crux of the matter – is crucial. That's where security people often fall down. That's where our communication needs to be sharper and more relevant.

“ Security professionals can always go to the nth degree in detail, but we've really got to know our audience. How do we sell our story and say ‘We need to invest money here, and in these resources’? It's not about scaremongering, it's about the reality of our situation.

“ Security people should learn to say, ‘We're trying our best to protect the organization, our stakeholders, our shareholders, our customers, and the people we employ. Now, with that in mind, let's talk about the threat landscape. What are we seeing out there? And why are these particular threats relevant to our organization?’

“It's also about saying, ‘Who are the largest revenue-generating organizations that we rely on? And, what are our biggest revenue-generating products? Now, let's see where threats could land in those spheres.’”

Where does the supply chain end?

But there are other challenges when your organization, and much of its supply chain, has become too technology-focused, he adds:

“ It’s tricky to talk about the supply chain when it comes to digital. For example, we might use Microsoft Teams, so Microsoft theoretically becomes part of the supply chain. You can define it at a basic application level.

“ But when you start thinking about your cloud services that might be hosted by Microsoft, that's a completely different footprint, a different story in terms of risk concentration. If Mr. Putin suddenly takes a dislike to Microsoft, then you've got a problem.

Outsourcing

“ Another challenge for a business like ours is that technology is so integrated in business processes and deliverables that it's hard to differentiate between who is a supplier and who is closer to being a functional department within our own organization.

“ Say product development is outsourced to an India-based development house, it feels like the same team working together: they're on the same email addresses, delivering to the same company values. If they are embedded, the distinction between vendor, supplier, and employee becomes blurred. That needs careful management.

“ As an organization, I don't think we've got it exactly right yet. Taking the example of a development house, you sign a contract and put expectations in. But how do you know that the product they're developing for you will remain secure?

“ How do you know that they're doing everything to make sure they're not bringing weaknesses into the products that you sell onto your customers? What assurances are they providing, and how are you holding them to account?

“It’s not just about trust: Don’t just trust, verify.”

Collaborative solutions

So, how challenging is it to work collaboratively when your organization is at the core of so many different relationships? How much of it is about insight, and where does that data come from?

“ There is so much available lessons now to help you see where you have weaknesses in real time. Or it can be third party penetration testing [pen-testing], or bug bounties, where you invite legitimate [white-hat] hackers to try to break your system.

“ But everything should be done on a risk-based approach: focus most effort where the greatest risk lies, take a tiered approach. Oversight is important, but you should also be able to challenge and hold vendors and other supply partners to account and say, ‘Show me that you're doing this properly.’”

The regulation angle

There is a regulatory dimension too, he explains – something of particular relevance in an industry, Financial Services, that is so heavily regulated:

“ We have conversations around operational resiliency. An industry regulator might say, ‘We think you are too reliant on one supplier, so you should de-risk yourself and split the cloud workload.’ But doing that is difficult, and you'll always need resources to keep up with expectations.

“ The most important point is that security isn't an add-on. It's part and parcel of everything you do. But that means it should be embedded right from the conception of a project, then that will filter through to the technology and tooling.”



Case Study: The multinational law firm

International law firms move in similar circles to Financial Services companies. However, they have daily processes and workloads that are, in specific ways, more people-centric: lawyers advise and represent their clients face to face, while handling reams of private data in both physical and digital forms.

That demands due diligence right across the supply chain, and not just in the digital elements of their extended enterprise, says the CISO of a major London-headquartered practice:

“ We issue an information security data privacy questionnaire to all our suppliers – infrastructure, SaaS and other cloud services, but also taxi companies, the people that supply flowers... everyone is assessed!

“ There are compelling reasons for having to scrutinize the security arrangements of our taxi company. They hold the names and addresses of our people, they drive them home, and we entrust them with our safety. That also means background and CRB or DBS checks [criminal record searches].”

Horses for courses

“ Of course, we hold different suppliers to different standards, such as anyone entrusted with sensitive information. There are technical controls that we would expect them to enforce, the use of encryption being one of them. It's whatever is appropriate for the service that they're delivering to us.”

As previously explored, attacks on trusted tools and applications are a growing feature of the cyber security landscape, which threatens to undermine organizations' own due diligence processes. He says:

“ We have a very tight turnaround for patching systems, if it's a critical or a high priority, we'll patch it immediately.

“ We also reject 80 percent of all emails that we receive, but there are things that remain difficult for anti-malware systems to spot, so some phishing emails still get through. But we use other sophisticated technologies, such as Content Disarm and Reconstruction (CDR). This creates a new, clean version of any document.

“ Plus, other systems root out malicious Web links. We use a proxy firewall service that has an intruder protection system [IPS] built into it. That's in addition to the detection and response software that we have on every computing endpoint as well.”

Focus on governance

In general, however, governance is the core part of the CISO job, he says:

“ We commit to maintaining [risk-based international security management system standard] ISO 27001. In addition to our internal audits, we do certification audits to validate that we have the right technologies in place, and that we are operating properly.

“ However, ISO 27001 is as much about the administrative processes as the technical ones. It is about the policies, the processes, and the training that we deliver to our users.

“ Training is a big part of the role. We deliver compulsory information security and privacy training to all of our users, once a year. We also deliver bespoke privacy and information security training to all business services departments and the practice groups. We issue lots of awareness and guidance.”

Conclusions

We are all working together as a team on that safe path through a forest of dangers. In this extended report we have explained the critical importance of collaboration, standards, agreements, and a stance of mutual strength rather than shared weakness.

Only by taking this approach can we avoid the butterfly effect. But it's worth asking: Why does the forest have to be so dense and full of risk in the first place?

Jordan LaRose, WithSecure™'s Director of Consulting and Incident Response, offers some final thoughts on the challenges of securing today's complex supply networks:

“ We are all more distributed these days, so it's harder for companies to enforce proper segmentation and proper network access. In technology terms, so many teams are moving to cloud-hosted platforms and to weaker authentication solutions.

“ Another change is in the code pipeline, with more and more organizations using public tools like GitHub. It is possible to lock it down, but

I would say it's insecure by default in terms of operational security. Instead of using an internal solution like GitLab, GitHub is just an easier way for developers to upload and manage code among themselves.

“ But solutions like that open more doors to attackers because, while the GitHub server might not be the actual attack vector, or even where they find a way to implant the backdoor, it might show them what the back end of a software package looks like.

“ This would give them an idea of, ‘OK, if I were to build a backdoor, how would I design it? And where could I insert it where it won't be seen but will be invoked, giving me reliable, easy access?

“ You can also see a laundry list of developers that have access to that repository. So, now you have a perfect set of targets to go after once you've got a foothold in the corporate network.

“ Now you can breach this guy's personal laptop, and from there all it takes is one login to GitHub, and that entire code repository can be compromised.

“ Similarly, with the open-source angle, it's not so much a by-product of distributed computing, but more a by-product of the dense ecosystem in which we find ourselves now.”

Think like an attacker. Collaborate as a team. And stay on the safe path with WithSecure™ to avoid the butterfly effect.



“‘Not a little thing like that! Not a butterfly!’ cried Eckels. It fell to the floor, an exquisite thing, a small thing that could upset balances and knock down a line of small dominoes and then big dominoes and then gigantic dominoes, all down the years across time. Eckels' mind whirled. It couldn't change things. Killing one butterfly couldn't be that important! Could it?”

– A Sound of Thunder, Ray Bradbury (1952)

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

