The complex world of supply chain security

Part 1: *Understanding the threat*

Executive Summary

Maintaining supply chain security is absolutely essential for organizations all over the world. And yet, it remains one of the most commonly misunderstood and overlooked aspects of the entire cybersecurity landscape. Given that more and more cyber criminals are targeting supply chains in order to bypass organizations' direct security defenses, why is it that awareness of the problem remains so disconcertingly low?

1. Cyber threats: the big picture

The worrying state of play

Last year the World Economic Forum revealed that cyberattacks are now the single biggest concern for businesses across Europe, North America and East Asia[1], outranking terrorism, unemployment and even failures of national governance in terms of their perceived significance.

This is understandable given the sheer volume of organizations being targeted. Successful cyberattacks cause all manner of operational, reputational or financial problems for the organizations concerned.

$2 trillion

The global cost of cybercrime expected to exceed in 2019[2]

32%

of UK businesses have identified cybersecurity breaches or attacks in the last 12 months[3]

197 days

The time taken to identify a breach, according to research from IBM

Overlooking the basics

It's fair to say that the cybersecurity industry has a tendency towards over-zealous headline grabbing when it comes to discussing cyberattacks. Commentators get hyperbolic whenever a new type of threat is identified – from crypto-mining to compromised IoT temperature controls, while savvy marketing teams have become adept at coining faintly ridiculous terms to describe them (think 'tailgating' or 'whaling').

However, **91%** of all targeted cyberattacks still occur via email, because it's still the preeminent form of business communication.[4]

You see, cybercriminals are not deranged computer nerds pursuing the art of creating the most pernicious pieces of malware the world has ever seen. No – they're in it to make a living, ideally in a way that requires least effort for maximum reward. In the same way that a burglar will always prioritize a wide-open front door over a heavily alarmed property, if a cybercriminal can continue to use the same old phishing techniques to extract money or credit card details from an unsuspecting email user, that's exactly what they'll do.

The right posture

In essence, this is what good cybersecurity is all about: closing off the easiest vectors of attack and creating a 'defense posture' that actively deters criminals from trying to attack you.

There are many such ways in which organizations can quickly and effectively bolster their email defense posture:

Internal protection
Deploy software that makes it harder for malicious emails to get through

Company training
Train your staff how to spot potential threats

External accreditation
Implement standards such as the NCSC's Cyber Essentials or the UK Goverment's Minimum Cyber Security Standard

You won't reduce the threat level to zero, because there is always the possibility – however remote – that a highly-motivated adversary or nation state with boundless resources behind it might target your organization and do whatever it takes to break in.

But by doing the basics well, you're signposting that it's going to take time and effort to break down your cyberwalls, and that would-be attackers are better off looking elsewhere for an easier target.

2. Recognizing the supply chain threat

The Achilles heel

With 33% of UK businesses now claiming to have documented cybersecurity policies in place[5] – up 6% in just 12 months – there's a sense that this pragmatic approach to cybersecurity, as advocated for by the UK's National Cyber Security Centre (NCSC) and the Department for Homeland Security in the US, is starting to catch on.

The only problem (and it's a big problem) is that far too many organizations are considering the problem in isolation from their wider digital ecosystems. They identify the threat posed by potential adversaries and try to stop those adversaries breaking in, but they don't take into account the likelihood of this occurring indirectly via their supply chain.

33% of UK businesses are now claiming to have written cybersecurity policies in place - up 6% in just 12 months

Almost all organizations rely on third parties in order to function, and this is becoming the Achilles heel of their cybersecurity operations. These third-party relationships could be for anything from the cleaning services they use to the servers on which they host their IT systems or the software they use to power their website.

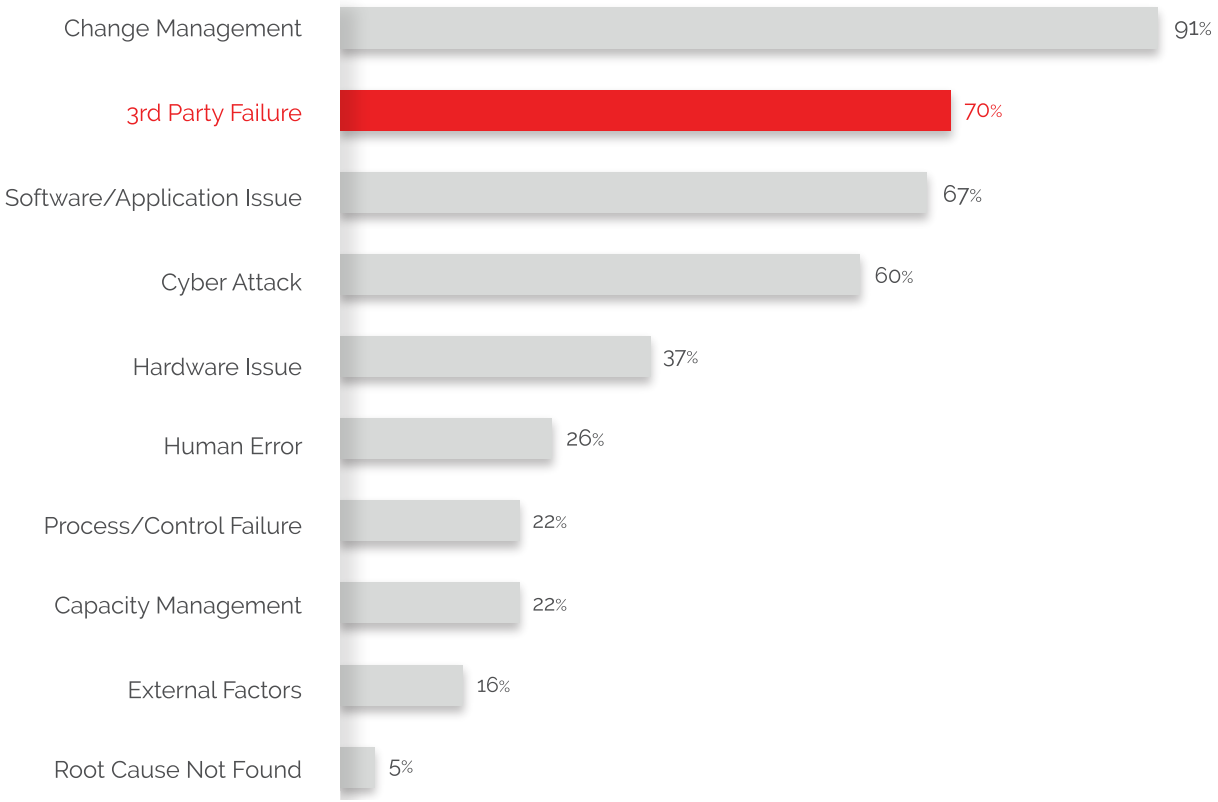
Understanding the nature of the problem starts with the phrase 'just suppose'. Just suppose you granted network login access to a website design agency partner so that they could directly access the graphics files and product information databases they required to complete your new website. And just suppose that a cybercriminal managed to compromise that supplier's own IT systems and steal those login credentials. Now you're compromised too.

Or just suppose the supplier you rely on for time management software has their software hacked and 'trojanized', meaning that when you download and install the new version of their software across your finance team, you've unwittingly introduced an unguarded backdoor into your network.

Research suggests that half of all cyberattacks on the business world now involve supply chains.

Hiscox's Cyber Readiness Report 2019 highlighted that **65%** of organizations had **experienced cybersecurity related supply chain issues** in the past year.[6]

According to the Financial Conduct Authority, most firms now rank cyber resilience as their top concern, with 'third party failure' cited as one of the three major weaknesses.[7]



This is not a hypothetical risk – **it's an active problem** that too many organizations are being blind-sided by while busy focusing their security efforts elsewhere.

Why is supply chain insecurity so prevalent?

The problem is seemingly one of trust. Organizations are rarely defrauded by third parties that they fundamentally distrust. If you distrust someone, you put up your defences and scrutinize them more intently – you certainly don't give them an all-access-pass to your business.

While supply chains are complex, sprawling and ever-changing beasts, each link is nevertheless comprised of a trusted relationship, and to date most organizations have focused their cybersecurity efforts on defending against untrusted outsiders rather than those on the inside.

There are four key errors that organizations will typically make with their partners:

1

The devil is in the detail

They don't ask new (or existing) suppliers for details of their security setup, so they have no idea if the suppliers pose a risk or not.

2

Make a list, and check it twice

They don't take steps to map out the true extent of their supply base or who has access to sensitive information. While many organizations have rules governing who is allowed to connect to the network and for what purpose, these tend to fall by the wayside once you lose track of who has access to your network or what they're supposed to be doing there.

3

Friends of friends

If organizations do mandate security provisions, these tend to apply only to immediate third parties rather than indirect suppliers across the wider supply chain, even where these indirect suppliers might actually pose a higher level of risk (e.g. if the project they are involved in is particularly sensitive).

4

Actions speak louder than words

The security 'vetting process' is a simple box-ticking exercise, such as a questionnaire and/or phone call to check everything is in order, rather than subjecting partners to genuine scrutiny or third-party penetration tests.

And of course, once the supplier has been approved, they usually stay approved indefinitely, even if their security procedures rust, decay or fall into disrepair. Even when these suppliers no longer provide services, many will just remain on the organization's systems, rather than being terminated. Few organizations require their supply chain partners to repeat the security provisions on a regular basis – head-scratching behavior when considering just how quickly cybersecurity threats continue to evolve.

This is everyone's problem

The challenges of supply chain security are complex enough when considering your own supply chain in isolation. The UK's National Cyber Security Centre declared that,

"Until you have a clear picture of your supply chain, it will be very hard to establish any meaningful control over it. You will need to invest an appropriate amount of effort and resource to achieve this."

National Cyber Security Centre
a part of GCHQ

But when we think about the fully interconnected nature of our digital ecosystems, it's easier to recognize the shared responsibility that everyone has to improve their security posture. We all exist in myriad different supply chains, which is why it's a mistake to consider the threat posed purely on the basis of the value of your own assets. If you're a supplier to Government, your own organization could be a useful avenue of attack for cybercriminals. If you're a supplier to a supplier to Government, you're still part of the Government supply chain.

3. What are the biggest risks?

Types of attack

Supply chain risks can vary wildly – from accidental or malicious activity by insiders within partner organizations, to external hacks by cybercriminals. They can also occur through simple miscommunication, for example, you communicate your security needs in a way that's unclear and so your suppliers end up doing the wrong thing and making mistakes.

The NCSC identifies four types of specific cyberattack carried out via organizations' supply chains:

Third party software providers

Criminals compromise the websites of software suppliers and replace their files with malware-infected versions, so that all of their clients unwittingly download them.

Website builders

Criminals target the website building tools used by creative agencies and compromise their code, so that their clients' websites do not behave in the intended manner.

Third-party data stores

Perhaps the most widely-understood threat, in which criminals hack the companies that aggregate, store and analyze sensitive data on behalf of their clients.

Watering hole attacks

Criminals specifically compromise a website that's frequented by users within a particular sector in order to deliver malware to everyone who visits it.

What's important to remember, however, is that the origin of each of these attacks is highly likely to be a targeted phishing email designed to induce an unwitting user into downloading malware or sharing sensitive company/client details. A scammer who compromises a machine on one company network may well be able to use it to infiltrate their partner organizations' networks too.

High-profile incidents

Over the last few years there have been countless incidents of major organizations suffering cyberattacks carried out via their supply chains, and it's worth examining a few of these to get a better sense of the typical tactics deployed by cybercriminals, as well as their ultimate motivations.

Attack Vector: Human error

Payload: Leak of personal data of 200 million voters

Cause: A small marketing company called Deep Root Analytics accidentally put the data on a publicly accessible server

2017
Date of incident

200 million
The number of records leaked by the political party

Attack Vector: Online rating system compromised

Payload: Leak of customer names and email addresses

Cause: The Australian subsidiary of Domino's suffered a security breach via an online ratings system supplier it had already ceased working with

2017
Date of incident

15,000
The number of hours of overtime from it's IT Staff to get the business running again

Attack Vector: NotPetya malware

Payload: The malware destroyed the firm's systems, cutting off its email and communications

Cause: The malware breached the law firm via a payroll software update from its Ukrainian accounting firm

2017
Date of incident

15,000
The number of hours of overtime from it's IT Staff to get the business running again

Attack vector: Asus Live Update tool hacked using Advanced Persistent Threat

Payload: Almost one million customers were hit with malware

Cause: Attackers were able to sign the malicious software with a real Asus certificate to dupe the customers into installing it

2018
Date of incident

1 million
The number of customers hit by malware

Attack Vector: Website compromised with malicious code

Payload: Millions of unsuspecting customers were duped out of their credit card details

Cause: The source of the attack has never been confirmed, but disclosed details point to a compromised piece of embedded code from a third-party supplier

2018
Date of incident

£183m
fine imposed by the Information Commissioner's Office (ICO)

Attack Vector: Individual employee computer hacked

Payload: Hackers made off with 100,000 photos of travellers and license plates belonging to the US Customs and Border Protection

Cause: A vulnerable Tennessee-based contractor, Perceptics, which has since been suspended from federal contracting

2019
Date of incident

100,000
The number of photos of travellers and license plates stolen

4. What's next?

We hope that you found this guide a useful introduction to the important and complex world of supply chain security.

We recommend you check out Part 2 of the Supply Chain Digest series Evaluating your supply chain for a clear and concise checklist of everything you need to know to identify a trusted and proven supplier for your organization:

- **Who's a supplier?** Drawing the line at the sandwich delivery guy
- **SME v Enterprise** - How do supply chains differ?
- **The MOT problem** - Why should you regularly evaluate?

Stay safe,

Team Red Sift

References

1. http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2018.pdf
2. https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security
3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
4. https://cofense.com/enterprise-phishing-susceptibility-report/
5. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_ Breaches_Survey_2019_-_Main_Report.pdf
6. https://www.hiscox.co.uk/cyberreadiness
7. https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf

Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at www.redsift.com

RED SIFT

Red Sift is a data-driven cybersecurity company on a mission to democratise the technology vital for organisations of any size or sectors to defend against security threats. Founded in 2015 and headquartered in London, UK, Red SIft boasts an impressive roster of international clients including TransferWise, Telefonica, Action for Children, and top law firms.

Products on the platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

www.redsift.com
contact@redsift.com
@redsift