Preparing for a cyber attack through your supply chain

January 2019

#IntelligentDigital

pwc.co.uk/cybersecurity

pwc

Global supply chains have become increasingly interconnected, causing a complex web of digital dependencies; this is making even the most security conscious organisations vulnerable. We are increasingly seeing attackers successfully exploiting these supply chain relationships in order to compromise organisations' critical networks and systems, and these attacks can have far reaching consequences. This paper seeks to raise awareness of this threat facing organisations across all industries, and highlights key recommendations.

Targeted attacks through the supply chain are on the rise

Cyber crime is a low risk, high reward activity, so it's hardly surprising that incidences of cyber crime are rising exponentially. As organisations improve their cyber security, those intent on breaching those safeguards have increasingly targeted the most vulnerable points. As supply chains have become increasingly interconnected and complex, they have quickly emerged as one of these.

56%
of organisations in 2018 have had a breach that was caused by one of their service providers[2].

35%
of companies in 2018 have had a list of all the third parties they were sharing sensitive information with[2].

Supply chains are an integral part of how businesses operate, heavily reliant on third party technology partnerships across cloud, data management, hardware, software and more. But these interconnected networks have made it increasingly difficult to manage vulnerabilities and threats at each stage of the supply chain. Even the most robust preventative controls can't protect organisations from motivated and highly funded threat actors, from organised criminals to state sponsored hacking groups.

The 'NotPetya' attack in 2017 is a prime example of the potential ripple effects of an uncontrolled targeted attack on the supply chain. By targeting accounting software used by a large number of organisations, cyber attackers were able to bring down critical operations and systems of businesses all over the world, resulting in millions of pounds in damage and lost revenue.

> "[A supply chain attack] is typically used as a first step out of a series of attacks. More concisely, it is used as a stepping stone for further exploitation, once foothold is gained to the target system."
>
> EU Agency for Network and Information Security[1]

Suppliers are a target

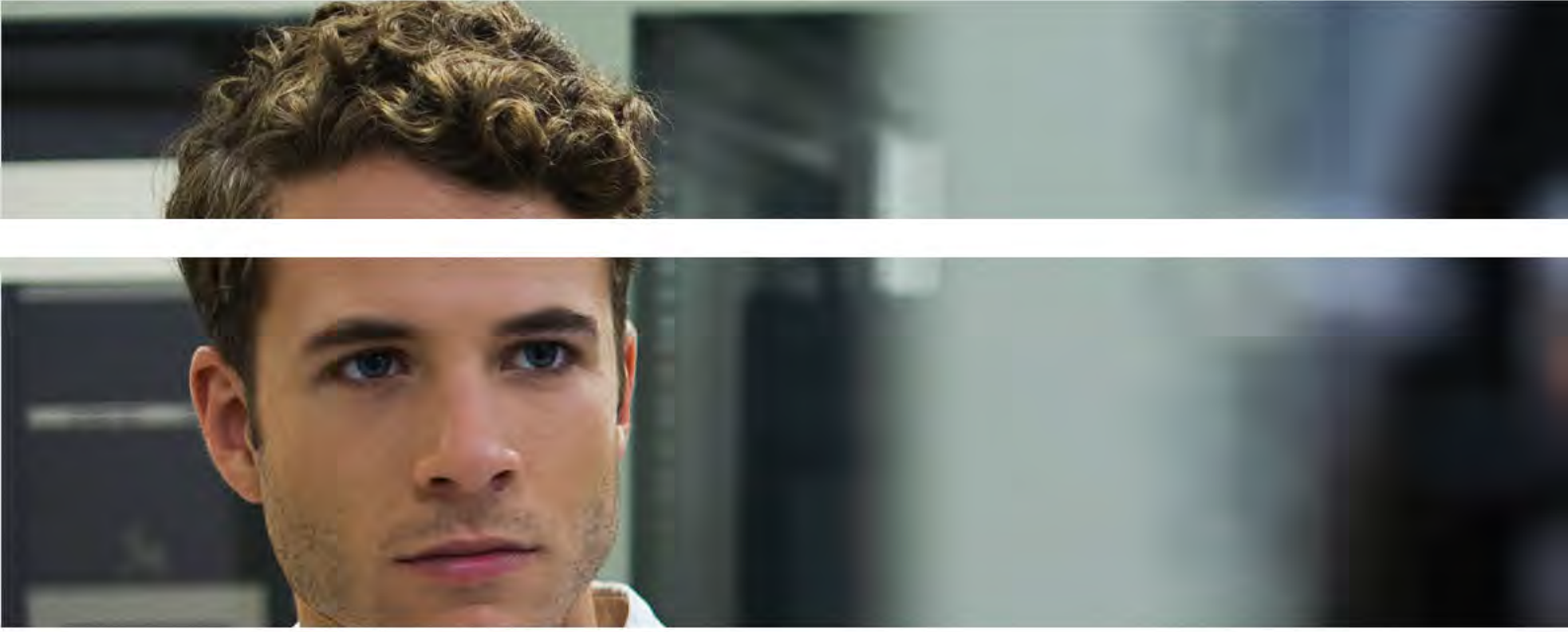
We're seeing a steady increase in large scale cyber attacks that target organisations by gaining a foothold into their suppliers, particularly IT infrastructure and software suppliers, which are often seen as an easier point of entry. Too many organisations fail to realise that their own data, intellectual property and systems are the real target of an attack on their supply chain. As a result, they leave the responsibility for managing cyber risks to their suppliers, rather than taking control themselves.

The implications of a supply chain attack are wide ranging and serious. Any attack on the supply chain has the potential to disrupt vital operations, threaten critical data and damage the relationship between an organisation and its customers and other stakeholders.

So what can you do to protect your organisation? Focusing on prevention is not enough for any type of cyber threat; you need a plan in place to detect, respond to and recover from a breach. But as supply chain based attacks increase in frequency and sophistication, it's essential to recognise the key factors that will manage the business risk.

[1] Supply chain attacks, ENISA, 2017: **https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks**

[2] What is a supply chain attack? Why you should be wary of third-party providers, CSO Online, 2018: **https://www.csoonline.com/article/3191947/data-breach/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html**



How supply chains are exploited

Through hardware

Hardware is a lot more difficult to update or replace in comparison to software and an attack through this vector can therefore have an even bigger impact. For example, the RottenSys malware campaign, identified by security researchers in early 2018, infected 5 million mobile phones worldwide with malware that was installed in the supply chain before delivery to end customers.

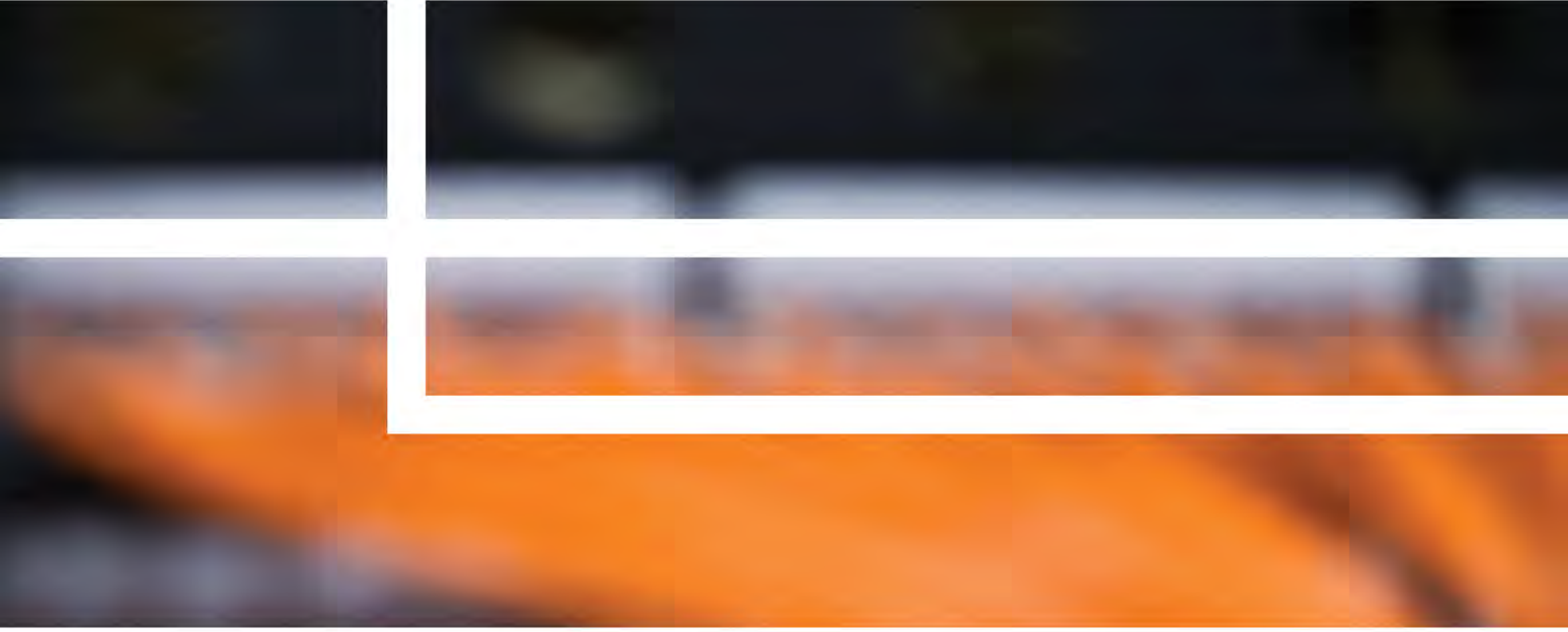
Through software

In 2017, hackers infiltrated a software company's network by compromising the download servers used to deliver a popular clean up application. The malicious software was masked as the legitimate application and downloaded by millions of users. This impacted global technology companies across the globe and resulted in the loss of critical data.

Through service providers

PwC and BAE Systems worked together to uncover and disrupt one of the largest sustained global cyber espionage campaigns ever seen, dubbed Operation Cloud Hopper and conducted by a threat actor referred to as APT10[3]. APT10 targeted managed IT service providers (MSPs) around the world, giving them access to the systems and data of both MSPs and their clients across more than 15 countries.

[3] Uncovering a new sustained global cyber espionage campaign – Operation Cloud Hopper, 2017: **https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html**



Preparing for a supply chain cyber attack

An attack on the supply chain is an attack on the end business. As targeted supply chain attacks become more sophisticated and prevalent, it's essential to be prepared to identify and manage the risks, and to have an incident response plan in place. Here are five key recommendations to help you be prepared to respond to targeted supply chain attacks:

Assess the security posture of your supply chain

The rise in targeted supply chain attacks has brought third party security into the spotlight. It's essential to understand each supplier's risk profile and how it aligns with that of your organisation, and its commercial priorities.

Organisations should carry out detailed third party risk assessments – covering not just technical security controls but governance, risk and compliance processes as well – and should define each supplier's level of maturity in these areas and identify any gaps in their security and risk management controls (and this should be an ongoing review process, rather than a one off exercise). This level of detail and visibility of suppliers' risks and operational data is essential to identify and put in place the right controls and processes that will allow you to respond quickly and effectively to a breach along the supply chain.

The procurement function should hold some of the responsibility for these assessments. Thorough due diligence on third party providers should be an integral part of the procurement process, and involve IT security from the beginning rather than as an afterthought.

Understand how you could be targeted through your supply chain

While it's not possible to prepare for every possible attack, some methods of attack are more common than others. Significant numbers of incidents, for example, involve attackers using techniques such as using legitimate credentials or exploiting unpatched software to gain unauthorised access to sensitive data. It is therefore vital to have a holistic threat view to inform your security and leadership teams of the types of attacks you should be preparing for.

To have a consolidated view of the threat landscape and specific threat groups, it is important to ensure a comprehensive threat collection and analysis strategy is in place. This means using a variety of open sourced, commercial and closed sources to build a broader picture of the threats you should be preparing for and enrich your internal security data. This threat view should be combined with a thorough understanding of your critical systems and data, as well as any identified gaps in visibility over the supply chain. With the help of this profiling and reporting, your security and risk teams will be in a better position to spot potential threats or vulnerabilities, including potential cyber attacks through your supply chain.

Consider applying this intelligence into your simulation exercises, such as red team assessments, to test your defences against multiple vectors of attack. This will help to identify areas of improvement across your business, including any opportunities to harden your defences and response plans for your supply chain.

Identify and secure the connection between your organisation and the supply chain

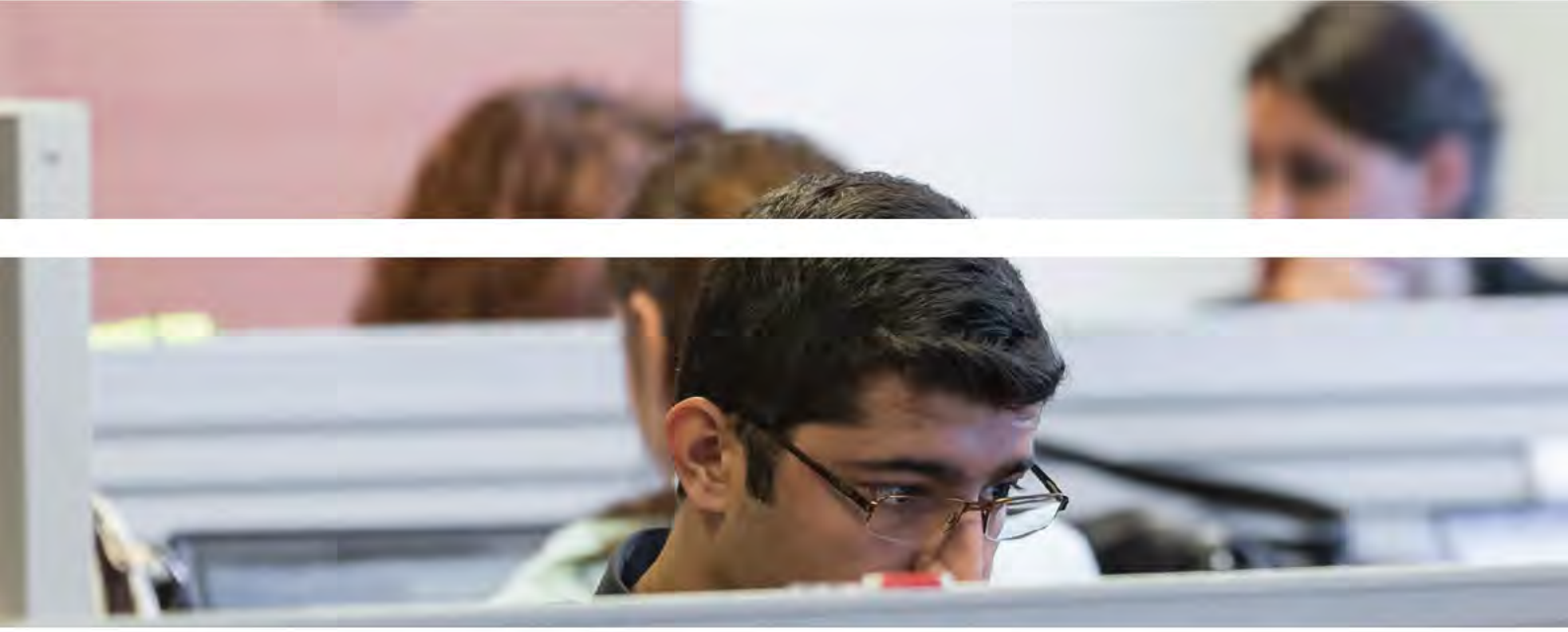
System architecture, and access and authentication controls, are all potential weak points in a supply chain and regular targets of cyber attackers. It's essential that your organisation fully understands the level of access that suppliers have to your environment. Do any systems have a backdoor built into products that allows remote access? If access is allowed, is the principle of least privilege applied?

In October 2018 the US Computer Emergency Readiness Team (US-CERT) issued an alert[4], following an increase in threat actors attempting to infiltrate the networks of global MSPs in a number of sectors, including energy, healthcare and manufacturing. This makes a number of recommendations designed to contain the movement of threat actors, including:

- using a dedicated Virtual Private Network (VPN) for MSP connection, and confining access to and from the VPN only to those networks and protocols needed (all others should be blocked, and failed access attempts logged),
- restricting the access of MSP accounts to only the systems they manage and disabling these when they're not needed, and
- ensuring MSP account passwords are aligned with the organisation's security policy.

We would also strongly recommend that a level of independence be maintained between providers of critical IT operations and incident response. While bundling the two services together may seem the most cost effective option in the short term, it is important to consider any potential conflicts of interest where that provider is effectively 'marking their own homework'.

[4] Alert from US-CERT, 2018: **https://www.us-cert.gov/ncas/alerts/TA18-276B**



Monitor, log, and analyse activity with your suppliers

Once you have established the connectivity and access your supply chain has to your environment, it's essential to monitor, log, and regularly review activity between your suppliers and your organisation. This will allow you to gain valuable insight that will help detect unusual or malicious activity.

You should identify a baseline for the normal activities between the supplier and your organisation. This makes it easier to detect and track anomalous behaviour. Logging and monitoring on all network systems and devices, and all endpoints, should be enabled, and logs stored safely in a central location (and backed up regularly). These logs hold invaluable information, however this will provide limited insight without using advanced analytical tools across the IT estate to inform your control decisions.

Where not already implemented, also consider capabilities such as unmanaged asset identification, asset security hygiene monitoring, and continuous threat hunting. Also consider broadening your threat detection capabilities or utilising a Managed Detection and Response (MDR) service which can help to spot malicious or unauthorised behaviour by bringing together advanced security technologies such as contextualised threat intelligence, behavioural analytics, proactive threat hunting and remote response.

Form a response plan

Incident management best practice adopts an end to end approach that covers readiness, response and recovery from both a technical and business perspective. The response plan should be organisation wide, addressing the actual and potential damage throughout the business, and updated and reviewed regularly. The roles and responsibilities, including decision making authority, of key stakeholders should be clearly set out, which will avoid a scattergun and inefficient approach to incident response where response decisions are required with little information and within short time frames. Four key areas that should be considered when forming a response plan should include at a minimum a process to coordinate the business wide response, communications planning, notifying regulators and recovery. These will be explained in more detail below.

In most cases a supply chain attack will be a board level issue, requiring rapid containment of disruption and damage, a swift assessment of impact and risk, professional and transparent communication with regulators and stakeholders, and orderly reparation.

The default response to a supply chain software attack for some companies is still to call in the IT experts – but a response that is IT based will only offer IT based solutions. The prevalence of supply chain attacks calls for a comprehensive approach to incident response that addresses both the technical aspects of a breach and the wider business risks, framed in the right way and using the right language.

If you choose to partner with an incident response provider, there are essential questions to ask:

- Does the provider offer rapid on site and remote response?
- Does it understand your IT environment and existing incident response processes?
- Does its team consist of both technical and business experts?
- Is it independent?
- Will it work with you to create a roadmap for incident response maturity, or only address events as they happen?

Consider a retainer with an industry leading incident response provider that is accredited by the NCSC's Cyber Incident Response scheme and can offer services that incorporate rapid response, effective preparation and expertise covering technical, business, legal, and privacy risks.

Determine your business response process

Cyber attacks present fully integrated risks to your organisation and cannot be managed alone by technical response teams. A cyber specific business response process is required to accommodate the speed, scale and uncertainty presented by cyber threats. This process will equip senior leadership with a foundation for efficient and effective response that identifies key impacts to be considered to support prioritisation, decision making and contingency planning.

Shape a communications plan

It is vital to the company's reputation and trusted relationships to have an aligned communications plan, one that can execute a quick, effective and consistent message to relevant internal and external stakeholders. Without a clear communications plan, the organisation risks not only damaging existing relationships but could also unwittingly reveal its vulnerabilities to opportunistic attackers.

The key internal and external stakeholders should be identified, along with the information that they will expect in the event of a breach. The business will need to be clear on what has happened in order to communicate the right messages; this will require collaboration between technical teams (incident responders or security teams) and non technical teams (the board, PR and legal teams).

Review your cyber insurance process

Cyber insurance gives organisations some comfort but should not be a cause for complacency. It's essential to understand exactly what the policy covers, and that you have the right controls and processes in place. In the event of an attack, insurers will look for evidence that the organisation had taken appropriate preventative measures, therefore it is important to ensure these are in place and not assume you are covered.

Some organisations are offered access to incident response providers as part of their cyber insurance policy, and these should be the subject of thorough due diligence. It is in the best interest of that organisation that they assess whether those incident response providers are accredited to respond to sophisticated attacks of national significance and include a high level of onboarding and preparedness services to ensure an effective and rapid response.

Prepare to deal with regulators

Navigating the regulatory landscape is a complex process at the best of times but in the wake of a cyber attack, it's essential to get it right. Regulations such as GDPR and the NIS Directive require organisations to notify their local regulatory body of a breach to personally identifiable data within 72 hours, or face significant fines. There have already been huge penalties exercised on well known brands; regulators will continue to make an example of others who don't comply.

A supply chain that involves cross border activity could mean dealing with more than one regulator. It's important to understand in advance what each regulator will expect and be prepared to respond to that. The Information Commissioner's Office, for example, has clear expectations around record keeping, transparency and communication. Are your documentation processes fit for purpose? Is a plan in place to communicate with regulators quickly and effectively in the wake of an event?

Reparation and data recovery

As well as addressing the immediate event, you will need to have a clear plan in place to recover from a breach in your supply chain. This should include, for example, prioritising systems so the business can get up and running again quickly in the event of a catastrophic event.

It is important to carry out incident response exercises that cover, wherever possible, the procedures for data recovery and reparation, and ask challenging questions of the organisation. Data may be backed up diligently but what would happen, for example, if your data storage solution was the target of an attack?

Conclusion

Organisations should be aware that an attack on the supply chain is likely to be more than just an attack on their suppliers. Targeted attacks are on the rise and organisations are increasingly being compromised through their supply chains. In our experience, the key to rapidly and effectively addressing a supply chain attack is to ensure you have the right people, process and technology in place to identify, manage and respond to these types of attacks. This includes:

- having a clear understanding of your supply risk profile,
- simulating what a targeted attack through the supply chain could look like to assess your capabilities,
- gaining clear visibility of data being transmitted between you and your suppliers so you can monitor and detect anomalous activity, and
- implementing a robust response plan that allows you to identify, detect, protect, respond and recover, with a strong understanding of how a business works.

Targeted supply chain attacks are a fact of life in the digital business world – but following these recommendations can be the difference between an incident turning into a crisis.

Contacts

Kris McConkey
Threat Detection & Response – Lead Partner
M: 07725 707360
E: kris.mcconkey@pwc.com

James Campbell
Incident Response – Director
M: 07565 844153
E: james.c.campbell@pwc.com

pwc.co.uk/cybersecurity

190110-143102-AI-OS