Cyber-security risks in the supply chain

Contents

Introduction

For any modern organisation, physical supply chain management already presents numerous complex challenges in understanding exposure to risk. The added complexity of cyber-security risks only amplifies this, regardless of their position within a supply chain. This paper provides an introduction to cyber-security risks within the supply chain, drawing on recent examples to highlight the benefits of an inclusive approach. It concludes with non-technical mitigation advice and points the reader to international standards for information security and management.

Intentional targeting and collateral damage

According to a Department of Business, Innovation and Skills report into information security breaches, 93 percent of large organisations and 87 percent of small businesses experienced a security breach in 2013, with affected companies experiencing roughly 50 percent more breaches than in 2012. [1] Many organisations struggle to protect the confidentiality, availability, and integrity of their networks and systems in such a rapidly evolving cyber threat landscape. Complex information and communication technology (ICT) services and support are often outsourced in an attempt to reduce infrastructure costs or streamline organisations. Almost every organisation experiences problems due to software or hardware malfunctions but typically these events are little more than inconveniences, although they have the potential to be devastating.[2] However, deliberate cyber threats may reach the organisation through any number of vulnerable points along the supply-chain.

When managing risks to their supply chain, modern organisations follow established procedures for mitigating dependencies and vulnerabilities that could impact upon their physical supply chains. These risks are identified, tracked, and assigned owners in a way which increases their visibility and allows organisations to anticipate their impact. However, this approach is seldom followed when dealing with cyber-security related risks to the supply chain and yet it is these risks that are most obscured, being several steps removed from the analysis and decision-making centre of a given organization.[3] As a result, they are displaced outside an organisation's control and an organisation may therefore find that, despite the

[1] Information security breaches survey 2013: technical report https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report
[2] Managing Cyber Supply Chain Risks, Advisen Insurance Intelligence http://www.advisenltd.com/wp-content/uploads/2013_OBPI_SupplyChainCyberRM_Whitepaper.pdf
[3] Cyber Security and the UK's Critical National Infrastructure, *Chatham House* http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0911cyber.pdf

strong cyber-security measures it has implemented through its ICT system, it has fallen victim to deliberate targeting or collateral damage.

The weakest link

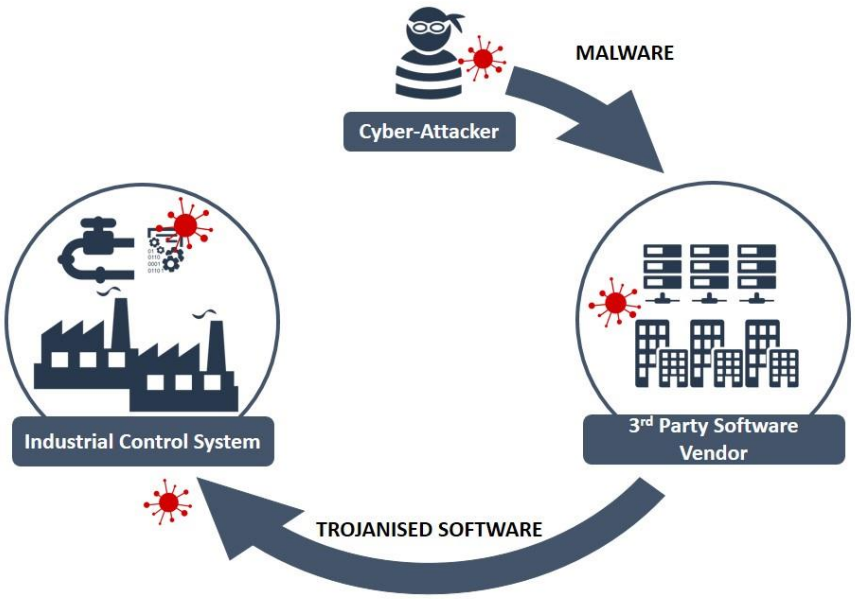
With information and security arrangements shared across a supply chain, the cyber-security of any one organisation within the chain is potentially only as strong as that of the weakest member of the supply chain. A determined aggressor, notably advanced persistent threats (APTs), will make use of this by identifying the organisation with the weakest cyber-security within the supply chain, and using these vulnerabilities present in their systems to gain access to other members of the supply chain. Whilst not always the case, it is often the smaller organisations within a supply chain who, due to more limited resources, have the weakest cyber-security arrangements. Small organisations accounted for 92 percent of the total number of cyber incidents analysed in Verizon's 2014 Data Breach Investigation Report.[4] They are often targeted because they are more vulnerable, represent a single point of failure, or have disproportionate access to important information given their size within a supply chain. This poses a particular risk for larger companies on whom they depend. The smaller firms they contract to produce the niche products required expose them to potential compromise regardless of their own cyber-security maturity.

[4] Verizon 2014 Data Breach Investigations http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

Recent examples of supply chain compromise

Outlined below are examples of recent supply chain compromises that illustrate the challenges organisations face and the mitigation that was taken.

Example 1: Third party software providers

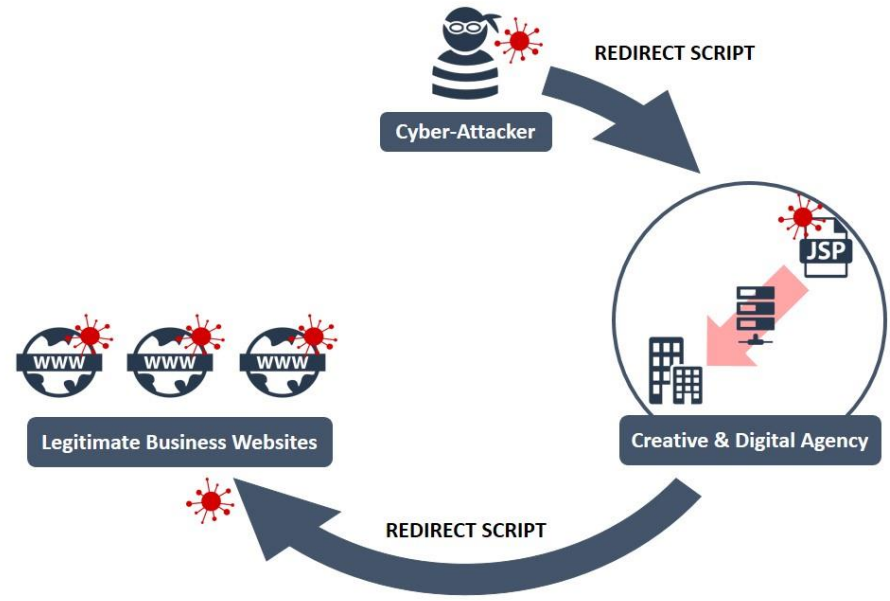


Example 1: Third Party Software Providers

Identified in mid-2014, the cyber-espionage group known as Dragonfly (also known as Energetic Bear, Havex, and Crouching Yeti) has allegedly been targeting companies across Europe and North America, mainly in the energy sector, since 2011. There is some speculation that pharmaceutical producers were the true target.[5] This group has a history of targeting companies through their supply chains, and in the latest campaign, Dragonfly was able to "trojanise" legitimate industrial control system (ICS) software. They were able to compromise the websites of the ICS software suppliers and replace legitimate files in their repositories with those that had malware added to them. The ICS software could then be downloaded from the suppliers' websites and install the malware alongside the ICS software. The malware included additional remote access functionalities that could be utilised to take control of the systems where it was installed. Compromised software is very difficult to detect if it has been altered at the source, and so there is no reason for the target company to suspect it was not legitimate. This places great reliance on the supplier, as it is not feasible to inspect every piece of hardware or software in the amount of depth required to discover this type of attack.

[5] Pharmaceuticals, Not Energy, May Have Been True Target Of Dragonfly, Energetic Bear http://www.darkreading.com/pharmaceuticals-not-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/d-id/1316869

Example 2: Website builders



Example 2: Website Builders

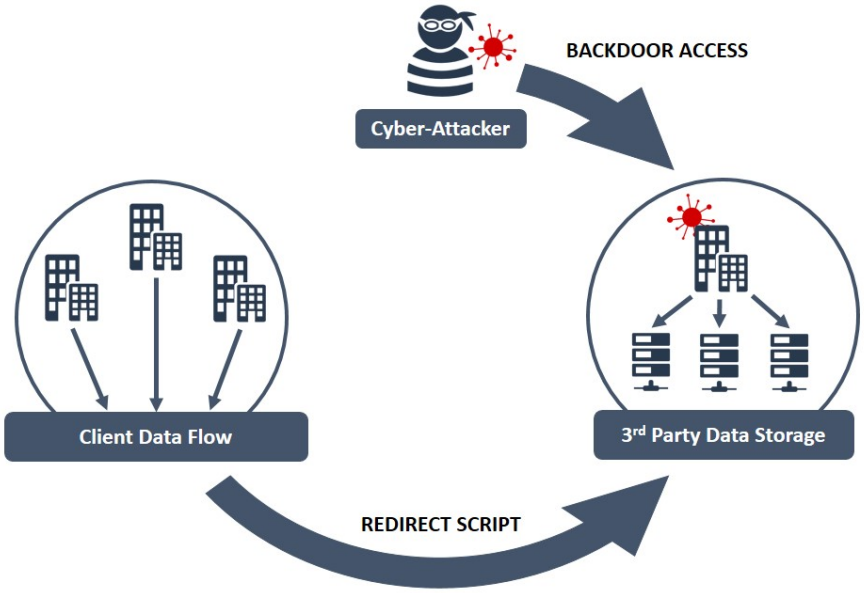
As well as cyber-espionage groups looking for commercially sensitive information, intellectual property, and critical vulnerabilities, cyber-criminals target supply chains as a means of targeting the broadest audience for their malware as possible. Identifying and compromising one strategically important element is an efficient use of resources and may result in a significant number of infections.

The Shylock banking Trojan is as a good example of this. Predominately focused on e-banking in the UK, Italy and the USA, those behind Shylock were disrupted and the threat from it reduced in July 2014 in a joint operation by law enforcement agencies and the cyber-security community.[6] The Shylock attackers compromised legitimate websites through website builders used by creative and digital agencies and employed a redirect script sending victims to a malicious domain owned by the Shylock authors. From there, the Shylock malware was downloaded and installed onto the systems of those browsing the legitimate websites. The economy of effort makes this a very successful endeavour. By integrating a multitude of different features adopted from other malware, Shylock was capable of performing customisable 'man-in-the-browser' attacks, avoiding detection and protecting itself from analysis.[7] Rather than compromising a number of legitimate sites individually, the attack

[6] 'Shylock' malware hit by authorities http://www.bbc.co.uk/news/technology-28245598
[7] http://info.baesystemsdetica.com/rs/baesystems/images/ShylockWhitepaper.pdf

targeted the core script of a website template designed by a UK based creative and digital agency.

Example 3: Third party data stores



Example 3: Third Party Data Stores

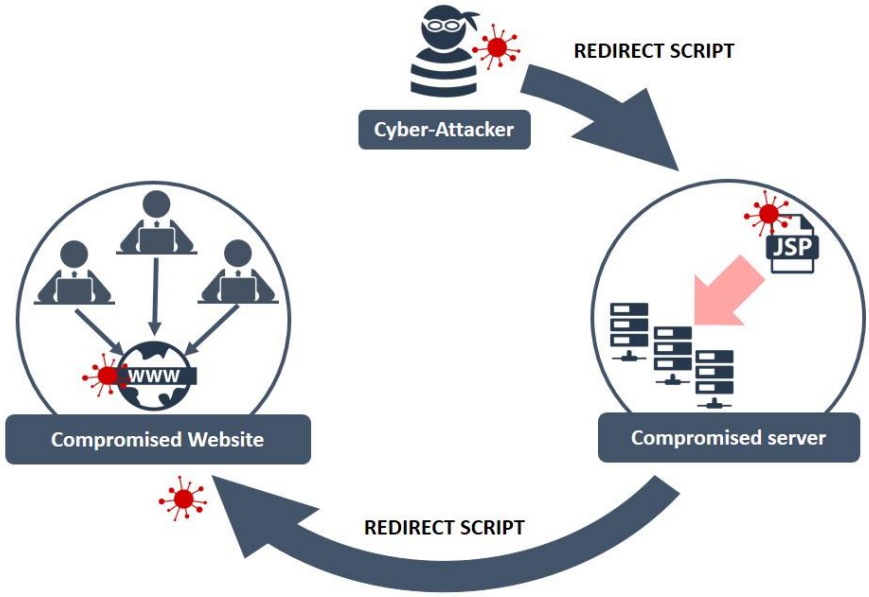
Many modern businesses outsource their data to third party companies which aggregate, store, process, and broker the information, sometimes on behalf of clients in direct competition. Such sensitive data is not necessarily just about customers, but could also cover business structure, financial health, strategy, and exposure to risk. In the past, firms dealing with high profile mergers and acquisitions have been targeted.[8] In September 2013, a number of networks belonging to large data aggregators were reported as having been compromised. A small botnet was observed exfiltrating information through an encrypted channel from the internal systems to a botnet controller on the public Internet.[9]

The most high profile victim was a data aggregator that licenses information on businesses and corporations for use in credit decisions, business-to-business marketing and supply chain management. While the attackers may have been after consumer and business data, fraud experts suggested that information on consumer and business habits and practices was the most valuable.[10] The victim is a credit bureau for numerous businesses and provides "knowledge-based authentication" for financial transaction requests. This supply chain

[8] Intro to Threats http://www.proofpoint.com/threatinsight/intro-to-threats/watering-hole.php; Hacking The Street? Fin4 Likely Playing The Market http://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf
[9] Data Broker Giants Hacked by ID Theft Service http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/
[10] Data Broker Giants Hacked by ID Theft Service http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/

compromise enables attackers to access valuable information stored via a third party and potentially commit large scale fraud.

Example 4: Watering hole attacks



Example 4: Watering Hole Attack

A watering hole attack works by identifying a website that is frequented by users within a targeted organisation or even an entire sector (e.g. defence, government, healthcare), and compromising that website to enable the distribution of malware. The attacker identifies weaknesses in the main target's cyber-security, and then manipulates the website chosen as a watering hole to deliver the malware that will exploit these weaknesses onto the target's system. The malware may be delivered and installed without the target realising (called a 'drive by' attack), but given the trust the target is likely to have in the watering hole site, it can also be a file that a user will consciously download without realising what it really contains. Typically the malware will be a Remote Access Trojan (RAT), enabling the attacker to gain remote access to the target's system.

Attackers are increasingly exploiting 'watering hole' sites by planting malware on websites deemed most likely to be visited by the targets of interest as a platform to conduct espionage attacks against a host of targets across a variety of industries.[11] The VOHO campaign is a good example of this. In mid-2012 a number of websites were hacked and silently redirecting visitors to another website. The hacked websites that were identified indicate the attackers focused on the organisations that were either in close proximity to the intended victims in

[11] Espionage Hackers Target 'Watering Hole' Sites http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites/#more-16707

Washington DC and Boston, Massachusetts, or were trusted websites familiar to the intended victims. Specifically targeted were the websites of a regional bank and a local government, along with websites relating to geopolitics, defence industry and education. Once these sites were accessed, the victims' systems downloaded the malware which consisted of a RAT that would allow extensive control of the system. Victims included education institutions, defence and technology sector organisations, internet service providers, health sector organisations, utility sector organisations, and state and federal government networks.[12]

Mitigation advice

The examples above highlight the difficulty of anticipating supply chain risks which arise from cyber-security related vulnerabilities. While there are usually three aspects to mitigation - centred on educating people, improving processes, and upgrading technology - cyber-security risks management within the supply chain is essentially an issue of trust. It requires a broad, inclusive approach allowing organisations to identify their place within the supply chain and map their cyber-security dependencies and vulnerabilities. This is often hampered by the following factors:

- The lack of a common risk vocabulary
- Inadequate data and information sharing across the supply chain
- Inappropriate or non-existent business resilience strategies

Critical business relationships must be graded according to the consequences of losing their services and be regularly reviewed for relevance and interactions between subsequent supply chain members identified.[13] Technically this is challenging and some of the most complex supply chains have so many external partners they may be unable to assess the risk of doing business with each one.[14] A number of other steps can be taken to ensure risk management is an explicit and integral part of supply chain governance.[15] The first is to institutionalize a multi-stakeholder supply chain risk assessment process that engages as many members of the supply chain as possible.

[12] Lions at the Watering Hole – The "VOHO" Affair https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/; The Voho Campaign: An in Depth Analysis https://blogs.rsa.com/wp-content/uploads/2014/10/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf
[13] Cyber Security and the UK's Critical National Infrastructure, *Chatham House* http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0911cyber.pdf
[14] Why Cybersecurity Is a Supply-Chain Problem http://www.supplychainbrain.com/content/blogs/think-tank/blog/article/why-cybersecurity-is-a-supply-chain-problem/
[15] Building Resilience in Supply Chains, *World Economic Forum* *http://www3.weforum.org/docs/WEF_RRN_MO_BuildingResilienceSupplyChains_Report_2013.pdf*

For small and medium sized organizations that are disproportionately exposed to cyber-security related risks, obtaining Cyber Essentials accreditation will contribute to their reputation as a well-defended partner in a supply chain[16] and will provide a solid baseline to improve upon. For large enterprises, the 20 security controls[17] combined with independent threat assessments will help identify cyber-security related risks to supply chains that provide demonstrable assurance of the processes and procedures of member organisations.[18] Ideally this would be coupled with technological platforms that allow estate monitoring and the intake of threat intelligence. This will not only improve an organisation's own supply chain risk management but also share threat intelligence with other organisations in the supply chain for a coordinated response. It is also important to get the basics right:

- Follow your procurement processes, evaluating cyber risk from the start
- Conduct thorough due diligence for new suppliers, accounting for their cyber-security competence
- Consider contractual clauses focused on security, stipulating responsibility for any compromise or data breaches and contractually mandate the flow down of security clauses to sub-contractor(s) in supply chain
- Challenge your suppliers to practice and develop collaborative processes for reacting to compromise or data breaches
- Conduct regular information assurance activity identifying critical pathways

Common standards and cyber-security risk management

The International Standards Organisation (ISO) produce the ISO 27000 series of standards, specifically written to address ICT security matters. ISO 27001 addresses process and auditing standards, which takes companies from basic risk assessments through to policies for managing information, communications, human resources, physical sites, business continuity and compliance.[19] Adopting the ISO 27000 series will further develop, harmonize and encourage the adoption of information security standards and go a long way to overcoming these. If this is adopted by every organisation in the supply chain along with the ISO 31000

[16] Cyber Essentials Scheme https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[17] Critical Security Controls guidance http://www.cpni.gov.uk/advice/cyber/Critical-controls/
[18] CREST http://www.crest-approved.org/news/crestcon-iisp-congress-2014-registration-goes-live/index.html
[19] Why Cyber security Is a Supply-Chain Problem http://www.supplychainbrain.com/content/blogs/think-tank/blog/article/why-cybersecurity-is-a-supply-chain-problem/

series (covering risk management), a common language for communicating cyber-security risks can be used throughout the supply chain.

It may seem a trivial point, but by implementing a common language with other members within its supply chain, an organisation can more easily anticipate, identify, communicate, and ultimately mitigate the risk posed by cyber-security related dependencies and vulnerabilities. The ISO standards are a framework for good security practice and, as such, are foundational. Once the standard is in place, it needs to be audited, maintained and then further technological and procedural steps taken to harden the environment often utilising perimeter defence technologies and logging and monitoring technologies such as security information and event management (SIEM). The importance here is not advocating the accreditation to international standards as these services can be commercially costly and as such can rule out their use in certain organisations. However, the importance is in their use by all firms in the same line of business: if the supplier and the supplied are both utilising and/or certified to the standard(s), then they share a common understanding of risk, information security and have a baseline set of measures in place that allows them to deal with the threat. Therefore, if both the supplier and supplied have a baseline level of security they are more resilient to the threat.

Summary

Supply chain risk management is challenging enough without considering the added complexity of ensuring sufficient cyber-security standards are implemented. The examples used here - third party software providers, website builders, data aggregators, and watering hole attacks - indicate how flexible attackers can be in their attacks. This has serious implications for organisations looking to improve their supply chain risk management. While there are multiple technical solutions and a number of common standards that can help to mitigate these risks, improving relationships amongst members of the supply chain is also very important for improving cyber-security within it.

www.cert.gov.uk

@CERT_UK

A CERT-UK PUBLICATION