FEATURE

The Missing Link in Assessing Cyberrisk Factors Through Supply Chains

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2DLe3SF

In February 2014, one of the biggest discount retailers in the United States, Target Corporation, reported a data breach within its network system that caused the leak of 110 million customers' financial and personal information. Target told reporters that the initial intrusion into its system was traced to network credentials that were stolen from a third-party vendor.[1] An investigation launched by the US Secret Service discovered that the attackers first broke into the retailer's network that previous November.

The hackers used network credentials to obtain access to Target's network, stolen from Fazio Mechanical Services, at the time Target's supplier for heating, ventilation and air conditioning (HVAC) and refrigeration systems. According to a US Senate report, "The vendor did not appear to follow broadly accepted information security practices,"[2] thereby allowing the attackers to compromise Target's network. Various sources have claimed the total cost of the breach as US $252 million and counting. With an offsetting amount of US $90 million in insurance proceeds, the total net expense comes to US $162 million.[3]

Ofir Eitan, CISM, CCSK, CTI
Is a cybersecurity manager at Leumi Card, the second largest payment company in Israel. He is former head of the Israel National Cyber Bureau Situation Room and acting head of the CERT-IL Hotline. Prior to that, Eitan served in the Israeli Intelligence Corps in various positions as an information security officer and a cyberthreat intelligence team leader.

Both Target and Fazio Mechanical Services stated that their IT systems and security measures were in full compliance with industry practices, noting that Target was compliant with the Payment Card Industry Data Security Standard (PCI DSS) at the time of the attack. This claim raised multiple concerns regarding Target's security architecture, design and mitigation efforts. For example, two security concerns arose. First, why did Target provide an HVAC company with credentials to the corporate network? Second, why did Target give the HVAC company access to a network that was not segregated from its payment system network?

In the wake of the Target breach, the threat of cyberattacks using an enterprise's supply chain as a delivery vector has become a common concern within the information security community. This has led to a significant increase in articles researching and analyzing supply-chain cyberthreats. Unfortunately, statistics show that any kind of vendor evaluation is still not widely in use among enterprises. For example, a cybercrime survey published in 2014 by the consulting firm PricewaterhouseCoopers (PwC) shows that only 53 percent of firms in 2013 had a process for evaluating third-party vendors. Surprisingly, the number dropped to 50 percent the following year.[4] Although years have passed since the statistics were published, it is unlikely that the number has changed drastically.

The increasing threat led to the publication of a framework by the US National Institute of Standards and Technology (NIST), which was updated in 2017.[5,6] According to NIST, any organization should identify, prioritize and assess suppliers and partners

of critical information systems, components and services using a cyber supply-chain risk assessment process. Moreover, in 2017, the New York State Department of Financial Services published the regulation 23 NYCRR 500,[7, 8] which is applicable to entities operating under the banking, insurance or financial service law in New York state. The new regulation instructs such firms to implement rigorous third-party cybersecurity risk management policies and procedures across the full life cycle of their relationship with third parties.

Nevertheless, the framework for a cyberrisk assessment of a vendor is still missing an important process. In this regard, a scoring method is necessary for defining the vendors that impose the highest cyberthreat to an enterprise. The methodology in this matter has certainly shown strong development in recent years, e.g., the demand to practice cyber supply-chain risk management (SCRM) monitoring and response.[9] However, risk assessment should first include a theoretical analysis based on a scoring method for defining high-risk vendors. This article offers such a scoring method to help information security managers protect against supply-chain cyberattacks.

> “RISK ASSESSMENT SHOULD FIRST INCLUDE A THEORETICAL ANALYSIS BASED ON A SCORING METHOD FOR DEFINING HIGH-RISK VENDORS.”

It is important to emphasize that a supply-chain cyberrisk can be imposed by an adversary or by an inside threat. Furthermore, any cyberthreat through a supply chain intrinsically means that the vendor has been hacked.

Step 1: Identify Assets

A proper risk assessment process starts with identifying essential assets that contain the enterprise’s critical information. This step is necessary before any mapping process takes place. Once the assets have been mapped, it is important to determine which assets are vulnerable to cyberattacks through supply chains and to classify them according to business risk and priority. Once finished, this process must be documented properly and approved by senior executives.

Step 2: Identify Enemies

As mentioned previously, supply-chain risk factors are characterized by the delivery vectors an attacker can use to hack into a network. Usually these hacks go undetected because supply-chain risk factors are often overlooked. The challenge is to balance the focus between possible delivery vectors and supply-chain risk factors.

The first step to identifying enemies is to consider the main cyberthreats that supply chains pose to an enterprise, such as:

- **Unauthorized remote access/authentication bypass**—Also known as unauthorized access control, this is the theft of a vendor’s credentials that grant remote access.
- **Malware insertion**—Also known as a web service attack, this is using or exploiting granted online access to a network through a vault or a removable-media gateway.
- **Compromising peer-to-peer (P2P) databases using Structured Query Language (SQL) injection**—This is a likely scenario when online access to a database is granted on an enterprise’s website.

- **Embedded backdoor malware**—This could be introduced through the components of programmable parts during the manufacturing process or during testing or loading of operation systems.
- **Denial-of-service (DoS) attack using P2P servers**—This can occur by launching a volume-based attack or an application-based attack (such as an XML attack) once an attacker compromises a vendor's network and the specific servers are in use.

Step 3: Define Important Vendors

An article published by the SANS Institute suggests that the first step toward building a vendor management program is defining the most important vendors.[10] The SANS article emphasizes the importance of classifying mission-critical vendors as high risk. Examples include the organization's important partners, financial and legal services, and hard-to-replace software vendors.

When it comes to delivery vectors for cyberattacks, the sensitivity of data shared with partners is not a key factor. On the contrary, what should be taken under consideration are the network accessibility mechanisms and the frequency of their usage by both the vendor and the employing enterprise. In other words, it is necessary to focus on the delivery vectors to the enterprise's network. More than any other criteria, this is the key to defining supply-chain cyberrisk factors.

Considering this paradigm, the scoring method described here encompasses the following factors to rate vendors:

- **File/code/access type**—This indicator is the core factor regarding the suggested scoring method. It goes without saying that this indicator corresponds directly with cyberthreats to supply-chain processes. Defining the relevant scoring to an enterprise involves a specific approach to every IT platform.

  Figure 1 presents a majority of the connectivity platforms of supply-chain processes that were described in step 2. A suggested scoring method is offered as well. Defining the highest scoring option to each ranked vendor is recommended.

- **Data-at-motion frequency**—Due to the online accessibility of services in a client-server model, this criterion does not often make a significant impact when it comes to assessing controls within an internal network.

  This indicator is very useful for defining an IT platform that is used to transfer data or to provide external accessibility, as such functions are frequently implemented for supply-chain processes. For example, an enterprise might not grant remote access to a specific vendor around the clock; however, the service might be available during predefined days or hours. The same applies for software code reviewing and examining components before implementation, the latter of which is executed offline.

> "WHAT SHOULD BE TAKEN UNDER CONSIDERATION ARE THE NETWORK ACCESSIBILITY MECHANISMS AND THE FREQUENCY OF THEIR USAGE BY BOTH THE VENDOR AND THE EMPLOYING ENTERPRISE."

  It is strongly recommended to use a distinguished scoring approach for this indicator. This means, for example, giving the highest score (5) to daily online connections (such as web services), a relatively high score (4) to a weekly application programming interface (API) update and a very low score (1) to occasional processes, such as the installation of a new system.

- **Number of delivery vectors**—As mentioned previously, it is highly recommended to base a supply-chain cyberrisk assessment on the delivery

Figure 1—Cyberthreats of Supply Chain Processes

Cyberthreat	File/Code/Access Type	Scoring	Comment
Unauthorized remote access/authentication bypass	Login authentication, VPN access, etc.	5	This gives direct access to a network, although the score should be defined according to its given credentials.
Malware insertion	Media gateway, P2P, etc.	4	It is recommended to distinguish between levels of policies such as connectivity platforms that grant the transfer of executable files (e.g., .exe, .bat) and those that transfer lower-risk files (e.g., .txt).
Compromising P2P databases using SQL injection/web service attacks	Data-driven applications, integrated web-based applications using open standards	3	Due to third parties frequently using these platforms, it is relatively common and easy for hackers to compromise these databases.
Embedded backdoor malware	Software/hardware implementation	2	While this cyberthreat is usually a risk to nation-state agents, it has increased for other groups recently due to deliberately implemented backdoors by worldwide IT enterprises.
DoS attack using P2P services	P2P gateway, integrating web-based applications using open standards	1	This is a rare threat due to a lack of interest and accessibility on the part of adversaries.

vectors to the enterprise's networks. Therefore, the number of both connectivity and gateway platforms is significant when one intends to define the highest-risk potential vendors.

As with the previous indicator, it is advised to embrace a distinguished scoring approach when it comes to scoring the amount of delivery vectors from a specified vendor. For instance, when it comes to cyberrisk, the difference between one delivery vector and four delivery vectors in total is enormous, whereas the gap between three and four delivery vectors is less significant.

To complete the scoring method, the appropriate best-practice equation(s) should be implemented:

- **Risk**—According to the known equation, risk equals severity multiplied by probability. In this case, regarding vendor definition, the risk should be normalized and, therefore, it equals the multiplication of file/code/access type, data-at-motion frequency and the number of delivery vectors.
- **Security controls**—Security controls are safeguards or countermeasures to avoid, detect, counteract or minimize risk factors to physical property, information, computer systems or other assets. The range of security controls is large and typically strongly tied to the enterprise and its network's characteristics. To fulfill the security controls criterion, one should execute sufficient business processes mapping, which should include the mapping of security controls related to the supply-chain processes.
- **Residual risk**—According to risk assessment best practices, residual risk is an assessment of the risk a supplier or vendor would impose after the analysis of the implemented controls, mainly from the information security realm.

Figure 2 presents the scoring method for assessing the residual risk that vendors may impose on an enterprise. **Figure 3** offers a blank scoring method for readers' own use, and **figure 4** provides a blank cyberthreats assessment for readers' own use.

Step 4: Planning the Security Program

Once the risk assessment process is complete, the next step is to consolidate mitigation plans as necessary regarding major vendors. This phase is strongly individual to the enterprise and, therefore, includes multiple considerations. It is imperative to use the best practices associated with each consideration. For readers seeking foundational knowledge about this phase, ISACA's Threats and Controls database[11] is recommended. The database's controls are categorized in six groups: architecture, data management, hardware, network, software and user management.

Figure 2—Supply Chain Cyberrisk Factors Scoring Method

Third Party	File/Code/ Access Type	Data-at-Motion Frequency	Number of Delivery Vectors	Risk	Security Controls	Residual Risk
John Doe and Sons Intel Services*	5	5	3	75	Two-factor authentication, antivirus software, sandbox environment, light security information and event management (SIEM) monitoring	55
Jane Doe Big Data Services**	3	4	5	60	API and service-oriented architecture (SOA) gateways, intense SIEM monitoring	35
Baby Doe Computers***	2	2	4	16	None	16

* A corporation has online data analysis using John Doe and Sons Intel Services Software as a Service (SaaS) platform. The services are provided using both multiple vaults for file transfer with the third-party supplier, and remote access is granted to the supplier to specific directories in the corporate network for file-editing purposes.

** The related customer consumes information offline from Jane Doe Big Data Services, using API web services to update various website databases on a weekly basis.

*** Baby Doe is the enterprise's main computer hardware and device supplier. There are no formal or *de facto* information security controls regarding the supplier. Therefore, neither firmware nor operation systems are checked before they are integrated with the corporate network.

Figure 3—Supply-Chain Cyberrisk Factors Scoring Method Sample

Supplier	File/Code/ Access Type	Data-at-Motion Frequency	Number of Delivery Vectors	Risk	Security Controls	Residual Risk

Figure 4—Cyberthreats of Supply Chain Processes Sample

Cyberthreat	File/Code/Access Type	Scoring	Comment

Conclusion

The bottom line is that cyberrisk factors through supply chains are evolving to be a major concern as part of the cybersecurity threat landscape. Although one can find plenty of sources and analysis covering this subject, there is still one framework missing: a scoring method for how to assess and define the risk of each of the third-party suppliers connected to the network. This article provides a comprehensive framework that covers this topic from a supplier-oriented perspective, as opposed to analysis focused on the attack vectors only. Therefore, this framework can be combined and integrated easily in a wider third-party risk assessment process, which analyzes both cyberthreats and the data leakage risk third parties might pose. To that end, the overall risk refers also to the risk of accidentally transferring sensitive data to a third party, in which case the supplier could be used maliciously as a delivery vector to the organization.

Endnotes

1 Krebs, B.; "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 2014, *https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company*

2 US Senate Committee on Commerce, Science and Transportation, "A Kill Chain" Analysis of the 2013 Target Data Breach," USA, 26 March 2014

3 Roman, J.; "Target Breach Costs: $162 Million," Bank Info Security, 25 February 2015, *https://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951*

4 PricewaterhouseCoopers, *The Global State of Information Security Survey 2015*, USA, *https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf*

5 National Institute of Standards and Technology, "Supply Chain Risk Management Practices for Federal Information Systems and Organization," SP 800-161, USA, April 2015

6 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, January 2017, *https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf*

7 New York State Department of Financial Services, *Regulation 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies*, USA, February 2017, *www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf*

8 Ernst & Young, *Cybersecurity Requirements for Financial Services Companies*, February 2017, *www.ey.com/Publication/vwLUAssets/EY-cybersecurity-requirements-for-financial-services-companies/$FILE/EY-cybersecurity-requirements-for-financial-services-companies.pdf*

9 National Institute of Standards and Technology, *Best Practices in Cyber Supply Chain Risk Management*, USA, *https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-FireEye-Cyber-SCRM-Case-Study.pdf*

10 Shackleford, D.; Combatting Cyber Risks in the Supply Chain, SANS Institute InfoSec Reading Room, September 2015, *https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252*

11 ISACA, Threats and Controls Tool, USA, 2017, *https://cybersecurity.isaca.org/csx-threats-and-controls*