Call for Supply Chain Security

Awareness of the risk to enterprise information assets through the supply chain surged after the 2013 Target Corp. data breach. Cybercriminals accessed 40 million credit and debit card accounts and 70 million customer personal-information records on the Target computer network through the corporation's local refrigeration systems supplier Fazio Mechanical Services.[1, 2] Increasing concern about lack of controls for the supply chain led to the expansion of cybersecurity frameworks, standards and requirements to enhance and better explain supply-chain risk management controls.

Suppliers are extensions of an enterprise's business. The supplier relationship management (SRM) governance area works to create a partnership between the enterprise and its suppliers. In cybersecurity terms, SRM ensures that suppliers have good cybersecurity hygiene. Following some sales-chain cybersecurity guidance and regulations can help ensure that organizations are compliant with security standards and regulations, and it ensures good supply-chain cybersecurity hygiene.

Cybersecurity Frameworks, Regulations and Standards

The US Health Insurance Portability and Accountability Act (HIPAA) Security Rule refers to suppliers as business associates.[3] The HIPAA Security Rule recognizes that the information security control requirements for hospitals also needs to be transferred to vendors and suppliers that do business with hospitals and other covered entities. The HIPAA Security Rule requires a hospital to have a business-associate agreement with each supplier to let the business associates know that they must meet the HIPAA Security Rule requirements. The business associates are contractually and legally obligated to protect the protected healthcare information (PHI) they handle when doing business with covered entities.

The US National Institute of Standards and Technology (NIST) greatly increased coverage of supply chain risk management in version 1.1 of its *Framework for Improving Critical Infrastructure Cybersecurity*[4] and in additional guidance found in Special Publication (SP) 800-161[5] and SP 800-53, rev. 4.[6] The explanations in section 3.3 "Communicating Cybersecurity Requirements With Stakeholders" were expanded to help users better understand cyberSCRM. The cyberSCRM property was added to implementation tiers, and the SCRM category was added to the framework core.[7]

The International Standards Organization (ISO)/International Electrotechnical Commission (IEC) added supplier relationships to its core security techniques standard ISO/IEC 27002:2013 *Information technology—Security techniques—Code of practice for information security controls*.[8] The standard requires enterprises to establish a supplier management program to ensure that all parties work in agreement to protect the confidential information that each party exchanges and possesses while conducting business.

Tom Bray, CISM
Is a business-driven cybersecurity leader with experience in banking, manufacturing, healthcare and technology. He enjoys working with organizations to align cybersecurity control capabilities with business objectives, improve cybersecurity governance processes and optimize investments in technical control tools. Bray is a contributing member of the West Florida Cyber Security Alliance and the ISACA® West Florida (USA) Chapter.

> “A GOOD SRM PROGRAM IS COMPLIANT WITH RELEVANT SECURITY FRAMEWORKS AND REGULATIONS AND ENSURES THAT SUPPLIERS HAVE GOOD CYBERSECURITY HYGIENE.”

The ISO 27002:2013 “Supplier relationships” section has the following requirements:

- **Information security in supplier relationships**—“There should be policies, procedures, awareness to protect the organization’s information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed upon within the contracts or agreements.”[9]
- **Supplier service delivery management**—“Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled.”[10]

The EU General Data Protection Regulation (GDPR) requires all entities, including subprocessors, to protect personal data. GDPR requires enterprises across the supply chain (i.e., data controllers, processors and subprocessors) to be managed as follows:[11]

- Identify all entities handling personal data (i.e., controllers, processors and subprocessors).
- Ensure that agreements exist for all subprocessors and that the agreements contain GDPR data protection obligations.
- Manage and audit subprocessors periodically, and provide evidence of their compliance.
- Include supply-chain partners in the enterprise data protection impact assessment (DPIA).

SRM Solution

A good SRM program is compliant with relevant security frameworks and regulations and ensures that suppliers have good cybersecurity hygiene. The considerations of a good SRM program include:

- Obtain and maintain senior management support and adequate resources to provide proper oversight of suppliers that handle sensitive information and/or access sensitive information via remote access.
- Ensure that supplier agreements have language that obligates suppliers to have minimum base-level cybersecurity controls in place.
- Establish clear agreement language on the type of data, such as personal data or intellectual property (IP), that will be exchanged with, stored and processed by the supplier.
- Provide data handling instructions, such as requiring data to be exchanged and stored in an encrypted format, limiting access to the sensitive data based on job role, and accessing attestations quarterly. Data handling instructions are often associated with the sensitivity level of the data or the data classification (e.g., internal use only, confidential, customer-confidential or restricted).
- Agree on the method to be used for the secure exchange of information, ensuring that all parties know that it is not acceptable to use public file-sharing sites.
- Obtain evidence from suppliers that they have the minimum base-level controls in place via:
  - Annual cybersecurity controls questionnaires that contain control evidence
  - On-site cybersecurity controls assessments every two years or alternating with annual control questionnaires
- Educate employees across the supply chain on the standardized secure file-transfer method, and ask employees to alert management if the agreed-upon secure file-exchange method is being circumvented.
- Host annual cybersecurity meetings with the supplier to collaborate and ensure that agreed-upon controls are working.
- Establish clear agreement language about what the supplier will do with the sensitive data after the relationship is terminated. An attestation of destruction is a common contract stipulation.

Conclusion

The information security of the supply chain is an increasingly important element of a holistic cybersecurity program. Suppliers are extensions of the enterprise. Therefore, enterprises are best served by establishing base-level data and system-control requirements for suppliers. Enterprises should have a process to periodically assess suppliers' compliance status.

Some supplier management programs provide suppliers with an annual scorecard that is based on the supplier's efforts to meet or exceed control requirements and compares scores with other suppliers. The scorecard can be a motivator for some suppliers and may have a positive impact on the supplier's future business with the enterprise.

Proactive supplier management programs take a partnership approach with suppliers and include quarterly supplier meetings. Successful meetings set a safe and friendly environment where information security challenges can be discussed openly, collaboratively and confidentially. With a partnership approach, all parties have a vested interest in the success of their joint efforts to secure data and information systems.

Endnotes

1 Kassner, M.; "Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned," *ZDNet*, 2 February 2015, *www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/*

2 Senate Committee on Commerce, Science and Transportation, "A 'Kill Chain' Analysis of the 2013 Target Data Breach," USA, 26 March 2014, *docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf*

3 US Department of Health and Human Services, "Summary of the HIPAA Security Rule," USA, *www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html*

4 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1*, USA, 10 January 2017, *www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf*

5 National Institute of Standards and Technology, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," SP 800-161, USA, April 2015, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf*

6 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," SP 800-53 Revision 4, USA, 22 January 2015, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

7 *Op cit* National Institute of Standards and Technology 2017

8 International Organization for Standardization (ISO), ISO/IEC 27002:2013, *Information technology—Security techniques—Code of practice for information security controls*, 2013, *www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en*

9 *Ibid.*

10 *Ibid.*

11 European Commission, EU Data Protection Rules, *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*