SAND2022-4430C

MANAGING CYBERSECURITY SUPPLY CHAIN RISKS FOR THE SECURITY OF RADIOACTIVE SOURCES

M.T. Rowland
Sandia National Laboratories
Albuquerque, NM, United States
Email: mtrowla@sandia.gov

Greg White
Lawrence Livermore National Laboratory
Livermore, CA, United States
Email: white6@llnl.gov

Trent Nelson
International Atomic Energy Agency
Vienna, Austria
Email: T.Nelson@iaea.org

Jacob James
Sandia National Laboratories
Albuquerque, NM, United States
Email: jacjame@sandia.gov

Abstract

Facilities with radioactive sources and their operations rely upon a complex arrangement of suppliers, vendors, and integrators to provide needed products, systems, services, and support. ISO 27036-1:2014 defines supply chain as "set of organizations with linked set of resources and processes, each of which acts as an acquirer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement". This linked set of resources and processes results in highly integrated products and services associated with significant cybersecurity risks.

Cyber-attacks targeting organizations through exploitation of their supply chain is an increasing trend that needs to be addressed in order to maintain security of radioactive sources. This requires the transfer of risks to suppliers and sub-suppliers with notification of vulnerabilities reported to operating facilities.

The management of cybersecurity (i.e., assignment to security levels; specification of computer security requirements) within cybersecurity programs at licensee facilities has historically been a complex process. Additionally, complex supplier and sub-supplier relationships, including free and open-source software where the providence may not be known, increases these challenges.

The current approaches involve standard terms of contract to apply specific measures, but these standard terms may be difficult to impose or assess their effectiveness within the organizations complete supply chain.

This paper outlines an approach for the cybersecurity supply chain through application of risk-informed approaches that apply a graded approach (i.e., security levels) and implement defense-in-depth (i.e., diversity, independence). The aims of this approach will be to improve (i) identification of risks; (ii) analysis of these risks and their potential impacts to the security of radioactive sources, and (iii) evaluation of risks to prioritize through contractual relationships and other countermeasures.

This approach aims to reduce the complexity of the current approaches by assigning cybersecurity requirements to a select set of suppliers and equipment associated with the greatest risks.

1. INTRODUCTION

Computer security is important for the protection of radioactive sources and the availability of operations utilizing these sources. Facilities using radioactive sources are growing increasingly reliant upon networked systems and digital infrastructure for monitoring and control over daily operations. This introduces an increased reliance upon suppliers, vendors, and integrators for the manufacturing, procurement, and construction of these systems. The network of external organizations that fall into these groups are the supply chain and represent a large attack vector for adversaries of radioactive source operations.

Adversary trends indicate that supply chains are increasingly being targeted by attackers. In the Global Security Attitude Survey by cybersecurity company CrowdStrike, 45% of respondents experienced at least one software supply chain attack in 2021, compared to 32% in 2018 [1]. The European Union Agency for Cybersecurity (ENISA) states "Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020 [2]. This trend drives the need for organizations to follow supply chain risk management (SCRM) best practices for their cybersecurity posture.

Computer security supply chain requirements have been introduced in nuclear security programs such as Nuclear Energy Institute (NEI) 08-09 [3], International Electrotechnical Commission (IEC) 62645 [4], IEC 63096 [5], and Canadian Standards Association Group (CSA) N290.7 [6]. While these standards apply to the nuclear power industry, supply chain cybersecurity is not unique to these operations, and in fact, measures from non-nuclear organizations may be considered for the U.S. NNSA's Office of Radiological Security (ORS). This includes the International Standards Organization (ISO) 27036 [7] and Energy Power Research Institute (EPRI) Cybersecurity Procurement Methodology [8]. ORS guidance currently covers procurement requirements in the Cybersecurity Procurement Requirements for ORS-Provided Systems [9], and supply chain has been identified as a risk to ORS systems in the Cybersecurity Best Practices for Users of Radioactive Sources [10]. Additionally, the IAEA has developed a draft publication on Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain [11]. However, these guides provide best practice guidance in the form of checklists, and not preparation and implementation of a supply chain risk management program.

This paper outlines an approach for the cybersecurity supply chain through application of risk-informed approaches that apply a graded approach (i.e., security levels) and implement defense-in-depth (i.e., diversity, independence). The aims of this approach will be to improve (i) identification of risks; (ii) analysis of these risks and their potential impacts to the security of radioactive sources, and (iii) evaluation of risks to prioritize through contractual relationships and other countermeasures.

2. SUPPLY CHAIN MANAGEMENT

The supply chain is the network by which a product or service moves from supplier(s) to the acquirer. Figure 1 below illustrates these relationships for a nuclear power plant supply chain.

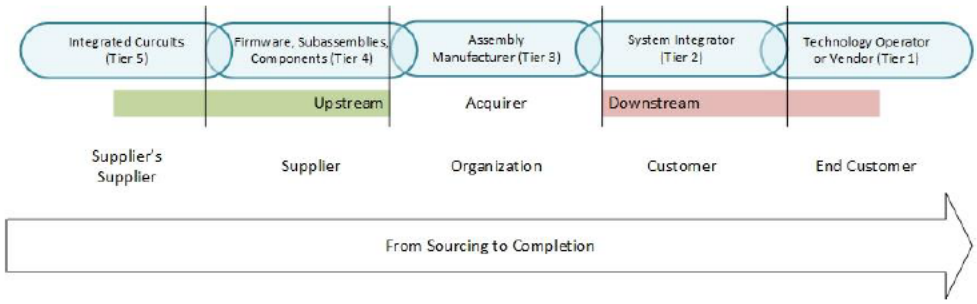

Figure 1. Supply Chain Relationships [11]

Relevant entities establish supply chain relationships with vendors, contractors and suppliers for a variety of reasons such as focusing resources on core functions; acquiring capabilities that the relevant entity needs but does not possess; acquiring a utility or basic service that is commonly available; enabling work from remote locations and acquiring new or replacement systems which perform functions related to nuclear safety or security [11].

An organization can have internal and external supply chain relationships. Therefore, supply chain risks are quite prevalent and the need for risk transfer (i.e., supply chain requirements) are necessary even if the supplier is within the same organization. For example, an organization operating facilities with radioactive sources may have operational and maintenance divisions that perform activities on the Physical Protection System (PPS). If cybersecurity risks of each of these activities are not identified or secure practices applied, there is a risk of a successful supply chain attack that exploits potential weaknesses resulting from differing practices that provide differing level of security.

2.1. Radioactive Source Supply Chain

Figure 2 is an example of a radioactive source licensee in which the licensee procures a sealed source and a physical protection system (PPS) to prevent unauthorized removal of the radioactive source. In this example, there are two supply chains: one for the PPS and the other for the radioactive source [11].

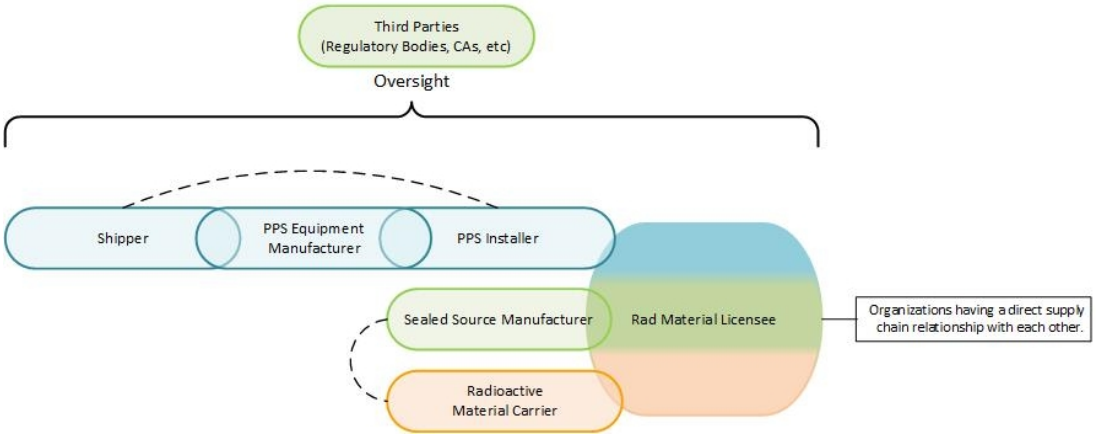

Figure 2. Example relevant entities relationships for radioactive sources [11]

As noted above, these supply chain relationships could be between internal or external organizations. Effective supply chain risk management need to account for all of these relationships. In Figure 2 above, there is a potential for compromise of the PPS system due to the activities of the Shipper, PPS Equipment Manufacturer, PPS Installer and the licensee (internal). These risks and associated attacks are further identified in the Supply Chain Attack Surface (see Figure 3 below).

3. RISK MANAGEMENT

Cybersecurity supply chain risk management follows a similar process to ISO/IEC 27005:2018 [13]. However, the major difference is that the risk transfer plays a larger role than the other risk treatment options. Risk transfer to the vendor or supplier is necessary because the vendor or supplier is most able to manage cybersecurity risk. The risk management process consists of the following steps (1) Risk identification, (2) Risk analysis, (3) Risk evaluation, and (4) Risk treatment.

ISO/IEC 27000:2018 [14] defines the four steps of Risk Management as:

- **Risk identification**: process of finding, recognizing, and describing risks.
- **Risk analysis**: process to comprehend the nature of risk and to determine the level of risk.
- **Risk evaluation**: process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
- **Risk treatment**: process to modify risk.

Effective cybersecurity risk management for the protection of radioactive sources demands additional inputs such as a threat characterization [15] and a site characterization. The threat characterization identifies and evaluates potential adversaries that are motivated to steal radioactive sources. Site characterization identifies and categorizes the functions such as physical intrusion detection and access control that allows for a graded approach to be applied when selecting and implementing controls.

The concept of a cybersecurity supply chain attack surface (SCAS) is also helpful to identify risks that may be associated with targeted attacks. For = radioactive sources, the PPS is a highly attractive target for cyber-attacks in support of physical intrusion attacks aimed at theft of the radioactive source. Targeted cyber-attacks related to radioactive sources are those that directly support theft of the radioactive source via degrading or disabling the physical protection system or sabotage operational technology devices that disrupt the benefits of the use of radioactive sources. The SCAS concept (see Figure 3 below) can also be leveraged for scenario analysis that can support analysis of vulnerabilities and weaknesses within the supply chain [16].

Specifically, important to cybersecurity for the protection of radioactive sources are the activities of (1) Hardware and Software Integration; (2) Testing; (3) System Integration, Provisioning & Customization; (4) Factory and Site Acceptance Testing; (5) Installation; (6) Maintenance and Upgrades, and (7) Repair and Return.

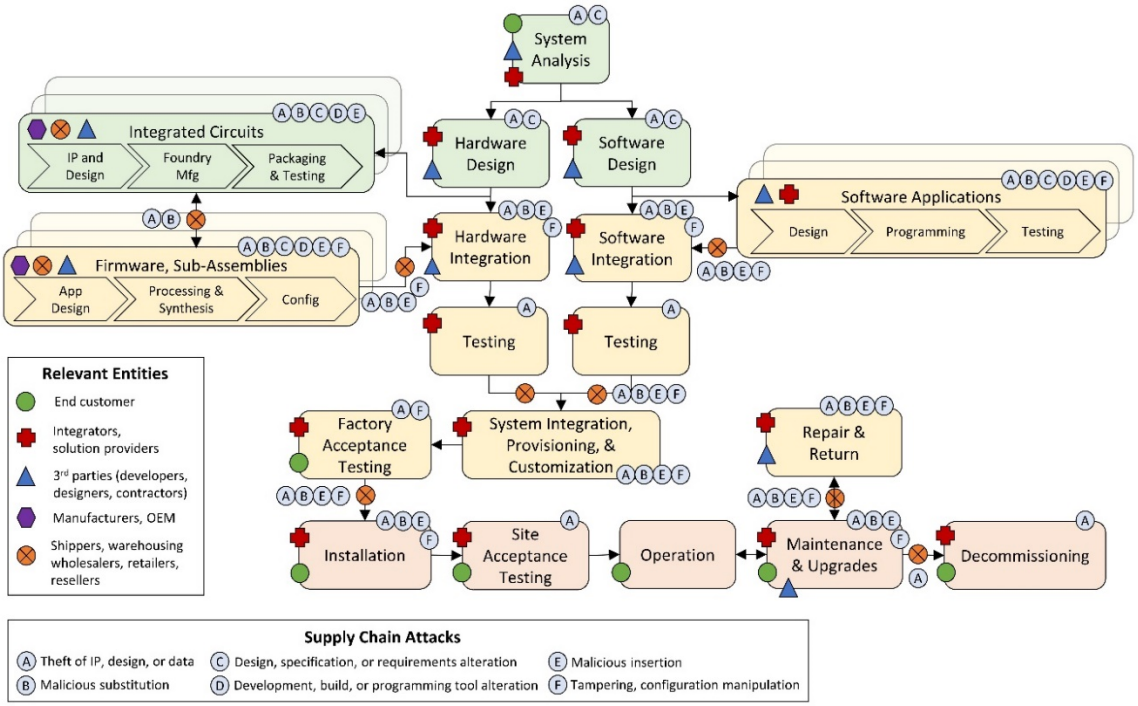

Figure 3 – Supply Chain Attack Surface [11]

4. SIMPLIFIED RISK MANAGEMENT EXAMPLE

This section will provide a simplified example for cybersecurity risk management for radioactive sources. The situation that will be considered are scenarios that can lead to theft of these radioactive sources.

In the both situations, the hypothetical hospital Gula[1] will be used to provide a basis for the analysis. A digital physical protection system (PPS) provides for security of the radioactive material. The radioactive source is used for blood irradiation and is located in the basement of the hospital. The PPS provides protection of this irradiator and alerts to a security monitoring room. The PPS is connected through a firewall to the site security system which then backs up key data to a cloud storage service.

4.1. Risk Identification

In the simplified example scenario of risks to the PPS, there is a risk from products and services. A small subset of these risks is provided in Table-1 below:

Risk No	Products/Services	Risk Type	Description of Risk	Applicability to PPS
1	Acquisition of Products	Information Security Feature	Acquirer's derived products, services, or processes vulnerable due to a supplied product's vulnerability	Vulnerability in the PPS HMI display software could allow for unauthorized disabling of alarms

[1] Gula is a hypothetical hospital that is leveraged by the IAEA for training and workshops on Nuclear Security.

Risk No	Products/Services	Risk Type	Description of Risk	Applicability to PPS
2	Acquisition of Products	Assurance	Without assurance, the acquirer may lack confidence in reliance upon the supplier's products	PPS Vendors that do not perform effective cybersecurity testing or provide patches to vulnerability
3	Acquisition of Services	Remote Access to in-house information and information systems	Supplier has remote access to information and information systems of the acquirer	PPS may require data from a human resource database which could allow an attacker to remote access into the database and pivot to PPS
4	Acquisition of Services	Processing of information offsite	Information under the responsibility of the acquirer is processed by the supplier offsite, using applications and systems under the control and the management of the supplier	Cloud storage of key data could give an attacker access by masquerading as someone that has access.

Table 1 Types of Supply Chain Cyber Risks [Adapted from [12]]

Threats to supply chain can be present in the vulnerabilities of an acquired product. This means that the security of an organization which acquires a product from a supplier could inherit risk from upstream of the supplier's supply chain. It is increasingly more common for organizations to rely on service models rather than to acquire products and build a capability themselves. Under the "as-a-Service" model, the end user needs to ensure proper identification of risk sources given the increased privileges they are allowing to external parties on their networks. As an example of an organization that needs to consider these risks, consider a hospital running a radiotherapy system. The requirements for operation of the machine require that it communicates to hospital servers and external cloud services, and has a physical protection system in place.

Following with the ISO/IEC 27005:2018 [13] guidance for risk identification, the following would be considered towards identifying risks:

Risk No	Risk Type	Description of Risk	Identification of Risk
1	Information Security Feature	Acquirer's derived products, services, or processes vulnerable due to a supplied product's vulnerability	**Identification of assets:** The primary system of interest is the blood irradiator in a teletherapy room in the basement. A PPS consisting of cameras, sensors, and door controls communicating with endpoints are in place to prevent physical intrusion. **Identification of threats:** The HMI in the Central Alarm Station (CAS) requires maintenance. The attackers have targeted the vendor's maintenance laptop that will be connected to the HMI computer. During maintenance, the vendor unwittingly installs ransomware on the HMI which targets the PPS sensors and controls. **Identification of existing controls:** A firewall is in place between the CAS machines and the PPS components to minimize the exposure of vulnerabilities to be exploited. **Identification of vulnerabilities:** The firewall is misconfigured and allows ransomware to propagate to the PPS components. An infected laptop could directly exploit the vulnerable (bypassing the firewall) through the portable media and mobile device connectivity with the PPS HMI. **Identification of consequences:** The malware disables (e.g., turns off) the PPS.
2	Assurance	Without assurance, the acquirer may lack confidence in reliance upon the supplier's products	**Identification of assets:** Same as previous. **Identification of threats:** Similar to previous, the attackers target the vendor's maintenance procedure. Being masqueraded as a legitimate update, the vendor installs malware that takes advantage of a vulnerability that allows for code execution on the target machine. **Identification of existing controls:** The firewall is in place between PPS components and HMI to minimize the exposure of vulnerable software to remote attacks. **Identification of vulnerabilities:** A version of software with known vulnerabilities that has not been patched by the vendor is running on the target machine. **Identification of consequences:** The malware provides the attacker with access to the HMI display, which they can use to change entries within the access control server such as the access control list to the blood irradiation room.
3	Remote Access to in-house information/ systems	Supplier has remote access to information and information systems of the acquirer	**Identification of assets:** In addition to previously identified PPS endpoints and components, an in-house server is used to store an Human Resources (HR) database. **Identification of threats:** Attackers gain access to the HR server on the unprotected side of the PPS firewall via remote connection and pivot to the PPS network as the HR server is a trusted endpoint. **Identification of existing controls:** A firewall separates the enterprise network from the PPS network. Authentication (i.e., username and password combination) is required for remote access for the HR server. **Identification of vulnerabilities:** Lack of IDS on the firewall. The HR server uses a simple method of authentication that can be easily overcome by adversaries. **Identification of consequences:** The adversary can obtain valid credentials to the HR server and perform a masquerade attack. The attacker may choose to disable or degrade the PPS access controls.

Risk No	Risk Type	Description of Risk	Identification of Risk
4	Processing of information offsite	Information under the responsibility of the acquirer is processed by the supplier offsite, using applications and systems under the control and the management of the supplier	**Identification of assets:** In addition to previously identified PPS endpoints and components, cloud storage is used to store sensitive key data. **Identification of threats:** Attackers gain access to the external party's cloud server and steal key data. **Identification of existing controls:** Authentication (i.e., username and password combination) is required for remote access for the cloud server. **Identification of vulnerabilities:** None identified at the facility. Authentication uses simple username passwords. **Identification of consequences:** The attacker uses stolen sensitive information to plan attacks with greater likelihood of attacks.

4.2. Risk Analysis

ISO/IEC 27005:2018 [13] considers both qualitative and quantitative risk methodologies.

Assessment of consequences: Considers business impact as a quantitative or qualitative, measurable value. Impact can be modelled in terms of monetary value, human impact, or time lost.

Assessment of likelihood: Given incident scenarios, likelihood calculations consider:

- experience and applicable statistics for threat likelihood;
- for deliberate threat sources: the motivation and capabilities, which change over time, and resources available to possible attackers, as well as the perception of attractiveness and vulnerability of assets for a possible attacker;
- vulnerabilities, both individually and in aggregation;
- existing controls and how effectively they reduce vulnerabilities.

Level of risk determination: Risk analysis assigns values to the likelihood and the consequences of a risk. These values can be quantitative or qualitative. Risk analysis is based on assessed consequences and likelihood. Additionally, it can consider cost benefit, the concerns of stakeholders, and other variables, as appropriate for risk evaluation. The estimated risk is a combination of the likelihood of an incident scenario and its consequences.

Incident Scenario for Risk 1

In this scenario, the adversary is aiming to disable the PPS through ransomware attack. This involves compromise of a PPS maintainer that has physical access to the PPS and performs updates by directly connecting a mobile device. The initial step is compromised of the maintenance supplier's networks via phishing attack. This provides the adversary with information on the PPS configuration and design as well as the schedule for maintenance activities. The adversary is then able to confirm vulnerabilities on the PPS that would allow for the installation of ransomware via the mobile device connection. The adversary waits until the ransomware is installed and then plans to commence a physical attack once the PPS is disabled.

Incident Scenario for Risk 2

In this scenario, the adversary's goal is to change entries in the access control list in a way that would go undetected by hospital staff. Once again, this involves compromise of a maintainer that has physical access to the PPS and performs updates by directly connecting a mobile device. However, instead of installing malware or ransomware on the target machine, the adversary exploits of a vulnerability present in software which has not been patched by the vendor. The attacker can deliver the exploit (an automated script to execute code on the target) by a phishing email to the vendor. The script would provide a backdoor for the attacker to connect remotely to the target, which would give them access to the HMI display which they can use to add themselves to the access control list for the blood irradiation room.

Incident Scenario for Risk 3

In scenario 3, the adversary's goal is once again to degrade the access control to the blood irradiation room by adding themselves or some false credentials to the list. The attacker gains initial access by exploiting a remote access vulnerability on a server used to maintain HR records. In order to escalate privileges on the server, the attacker needs to authenticate as a valid user. By a brute force attack, the attacker discovers a weak password that is used to authenticate. Because the firewall lacks intrusion detection, the attacker is able to pivot to the PPS network undetected. Once on the PPS network, they can add themselves to the access control list for the blood irradiation room.

Incident Scenario for Risk 4

In this scenario, the adversary aims to gain access to sensitive data in cloud storage. The external party that manages the cloud does not enforce strict password policies, and the attacker takes advantage by brute force attack. Once authenticated, the attacker has access to sensitive information (e.g., video data) which can be used during the reconnaissance stage of the attack on the PPS system, increasing the likelihood of attack success.

Risk No.	Risk Type	Identified Risk	Likelihood	Consequence
1	Information Security Feature	Attackers use maintenance on the PPS HMI to disable PPS.	Low Phishing and ransomware attacks highly probable. However, leveraging these attacks to target PPS of other RM have yet to be reported.	Low The PPS system fails secure, so an attempt to completely disable the system would not provide access. The failure is detected in a relatively short period of time and the compensatory actions are known (e.g., guards at entry points).
2	Assurance	Attackers use an unpatched vulnerability on the HMI machine to add themselves to the access list for the room.	Medium Phishing and ransomware attacks are highly probable. The attack assumes the target machine is vulnerable to malicious code execution, which the attacker cannot verify prior to launching the attack.	Medium The attacker could change the access control list, masquerade as an authorized employee and remain undetected until the next audit of the list.
3	Remote Access to in-house information/ systems	Attackers gain access to the HR server via a web interface and pivot to the PPS network.	Low Remote access to a server (e.g., through a web interface) is a legitimate threat. If strong password policies, periodic renewal, and dual-factor authentication are not enforced, then a brute force attack could be possible but time consuming. Leveraging these attacks to target PPS of other RM have yet to be reported.	Medium The attacker could change the access control list, masquerade as an authorized employee and remain undetected until the next audit of the list.

4	Processing of information offsite	Attackers gain access to cloud storage of key data and use stolen keys to gain access to the room.	Low Performing a dictionary attack informed by open source breaches of accounts on a site that has weak authentication is possible and may be time consuming, but this is the only step in the attack.	Very Low The disclosure of information makes a subsequent attack on the PPS system more likely, but does not directly harm the PPS. The information acquired is not assumed to be highly sensitive. The adversary may be able to acquire this information through other means.

4.3. Risk Evaluation and Prioritization

The following is the list of prioritized risks (ordered from most to least significant) based on the simplified risk analysis above:

1. Risk 2 (Assurance)
2. Risk 3 (Remote Access to in-house information/systems)
3. Risk 1 (Information Security Feature)
4. Risk 4 (Processing of information offsite)

These risks may change as additional credible incident scenarios are analysed. The expectation is that the severity of consequences will relatively constant for each risk independent but the likelihood of the scenario will vary.

4.4. Risk Treatment

Risk Treatment for supply chain generally involves (1) Risk Transfer to the supplier via contractual requirements (external) or via policy or organizational requirements (internal); or (2) Risk Modification such as cybersecurity tests and checks before, during or after the supply chain activity.

For each of the prioritized risks, the following are potential risk treatment options:

Risk 2 (Assurance; highest priority):

Risk Transfer: Contractual Requirements to demonstrate cybersecurity tests and assurance, communication of vulnerabilities and patches, auditing of cybersecurity programme of the supplier. The overarching objective is to demand and verify greater effort by the supplier(s) to provide security assurance. For instance, the absence of patches does not imply effective security management (i.e., no vulnerabilities) but more the converse. The additional requirements will likely add to cost, but given that this is the highest priority risk to treat, a persuasive business case could be made.

Risk Modification: Knowledge-based detection (for known malware, vulnerabilities) would be effective in limiting the risks to targeted attacks. However, the risk of targeted attacks leveraging this weakness is not negligible. Therefore, behaviour-based detection that requires continuous monitoring might be necessary (e.g., Cyber SOC, host-based intrusion detection). Defensive Computer Security Architecture (DCSA) elements that prevent the establishment of Command and Control (C2) Channels would also be effective in minimizing the potential impacts of the scenario. The consideration of the costs and benefits of solutions that provide for continuous monitoring will be examined in the case studies.

Risk 3 (Remote Access to in-house information/systems):

Risk Transfer: Contractual requirements to demand the use of complex passwords that are periodically refreshed. Awareness and specialized training for persons provided with remote access. Audit and Assessment of the effectiveness of the supplier's cybersecurity program (e.g., phishing campaigns).

Risk Modification: Requiring complex passwords with multi-factor authentication. Continuous monitoring and alerting for attempts to exploit remote access.

Risk 1: (Information Security Features)

Risk Transfer: the same requirements above apply, however possibly less aggressive.

Risk Modification: Assessment and review of patches or vulnerabilities. Defensive Architecture elements that limit or mitigate the attack pathways that would allow for attacks that could exploit the vulnerabilities.

Risk 4 (Processing Information Offsite)

Risk Transfer: for sensitive information, a public cloud where the service is accepted "as-is" does not allow for the necessary requirements to be imposed on the cloud service provider. However, in this case the information backed up to the cloud is not particularly sensitive (not assumed in this case), so the risk may be acceptable.

Risk Modification: Require multi-factor authentication for access to the cloud. Require the use of encryption prior to back up to the cloud.

5. SUPPLY CHAIN ATTACK CASE STUDIES

The importance of controlling the supply chain attack vector for ORS facilities is evidenced by adversary trends observed by organizations. In recent months, attacks against IT and OT systems have increased. The following sections outline two recent events in which adversaries exploited the supply chain attack vector. The SolarWinds attack demonstrated how a supply chain vulnerability could be exploited for a wide-spread attack across many customers and industries.

5.1. SolarWinds Breach – SUNBURST Attack

Founded in 1999, SolarWinds is a company headquartered in Austin, Texas with roughly 300,000 customers worldwide [17]. In December 2020, the cybersecurity firm FireEye discovered and disclosed an attack on their organization [18]. The attack leveraged the SolarWinds product Orion, which is used by organizations to act as a single platform responsible for management and monitoring of IT systems (networks, servers, applications, logs, etc.). FireEye discovered the attack when an independent, in-house developed system noticed anomalous system administration activity. They continued to investigate and discovered that their proprietary Red Team tools were stolen and exfiltrated. FireEye discovered that the exploit was able to perform file transfers, execute files, and disable system services [19]. Figure 4 illustrates the SolarWinds attack timeline.

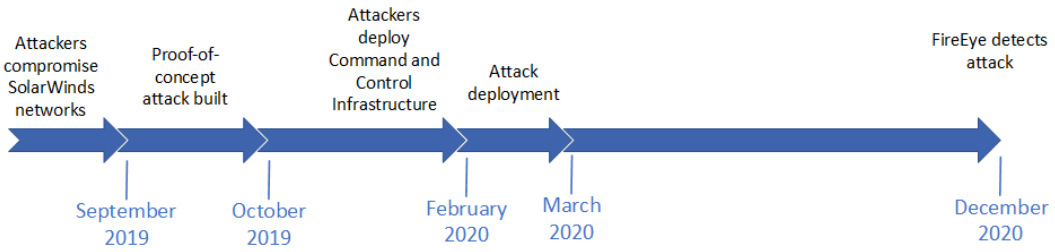

Figure 4: SolarWinds attack timeline.

The SolarWinds breach targeted the early stages of the software development process, far upstream in the supply chain for many of the attackers' targets. By modifying a legitimate Orion plug-in with a digitally-signed backdoor, attackers were able to ensure that trojanized code passed security checks performed by the SolarWinds development teams and customers receiving the malicious version updates. The network access that the attackers achieved gave way to additional supply chain compromises for organizations that were not SolarWinds' customers. One example is cloud and email security firm Mimecast, which revealed that the SolarWinds attack allowed attackers to compromise code bases and certificates used to authenticate LDAP, Azure Active Directory, Exchange Web Services, POP3 journaling, and SMTP-authenticated delivery routes for their customers [20]. This relationship is demonstrated in Figure 5 below.

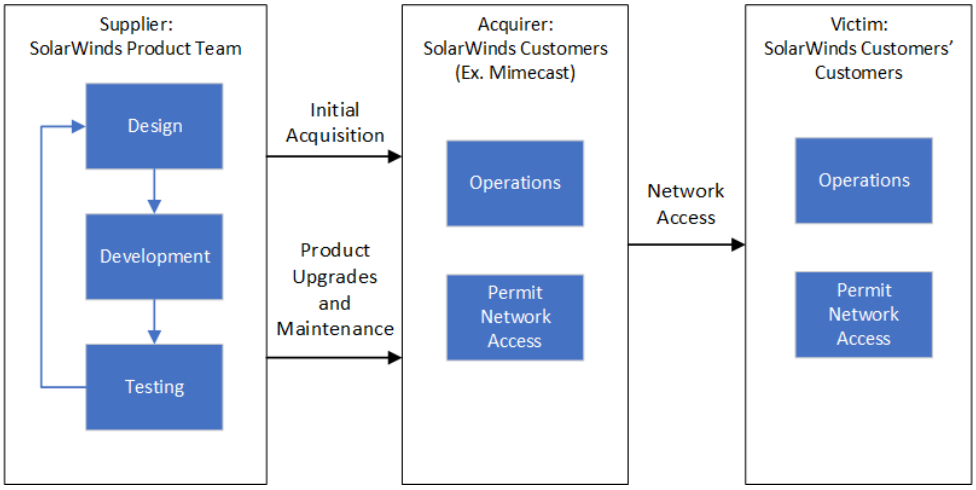

Figure 5: SolarWinds supply chain propagation.

5.2. SolarWinds ORM Supply Chain Risk Analysis

The two risks identified in the simplified risk assessment are Risk 2 (Assurance) and Risk 4 (Processing Information Offsite). Most of the Risk Transfer arrangements for Risk 2 described above would have directly minimized the potential for this attack to be successful. However, given the capabilities of the attacker, it is unlikely to have completely prevented this attack. Therefore, significant effort to implement independent continuous monitoring and DCSA elements to prevent C2 Channels would have likely detected the attack (assuming that a good baseline of PPS behaviour has been characterized) and mitigated via DCSA elements. However, Risk 4 may have allowed some information to be obtained by the adversary utilizing this attack.

6. DEFENSE-IN-DEPTHCONCLUSION

This paper outlines an approach for the cybersecurity supply chain through application of risk-informed approaches that apply a graded approach (i.e., security levels) and implement defense-in-depth (i.e., diversity, independence). The aims of this approach will be to improve (i) identification of risks; (ii) analysis of these risks and their potential impacts to the security of radioactive sources, and (iii) evaluation of risks to prioritize through contractual relationships and other countermeasures.

A simple risk management process with a few incident scenarios demonstrates the effectiveness of supply chain risk management leveraging the multiple approaches [11, 12, 13]. In many cases the risk treatment options of risk transfer (through contractual requirements) and risk modification (in house security controls and practices) provide defense-in-depth against many supply chain attack attributes as demonstrated by the case study analysis. With the risk of supply chain attacks increasing, greater effort should be applied to assist licensees in developing approaches and implementing best practices as detailed in ORS guides [9, 10].

ACKNOWLEDGEMENTS

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

REFERENCES

[1] CrowdStrike, "What is a Supply Chain Attack?", 8 December 2021. Available at https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

[2] ENISA, “Threat Landscape for Supply Chain Attacks”, 29 July 2021. Available at https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
[3] NEI, “Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 (Rev. 6),” Washington, DC. (2010)
[4] IEC, “Nuclear Power Plants – Instrumentation, Control, and Electrical Power Systems – Cybersecurity Requirements, IEC 62645:2019,” IEC, Geneva. (2019).
[5] IEC, “Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Security Controls, IEC 63096:2020,” IEC, Geneva, (2020).
[6] CSA, “Cyber Security for Nuclear Facilities, CSA N290.7-21,” CSA Group, Toronto, (2021)
[7] ISO/IEC, “Information Technology – Security Techniques – Information Security for Supplier Relationships – Parts 1 through 4” ISO/IEC 27036, ISO, Geneva, (2013-6)
[8] EPRI, “Cyber Security in the Supply Chain: Cyber Security Procurement Methodology, Rev. 2, EPRI Technical Report 3002012753,” EPRI, Palo Alto, (2018).
[9] ORS, “Cybersecurity Procurement Requirements for ORS-Provided Security Systems,” ORS, Washington, DC, (2018).
[10] ORS, “Cybersecurity Best Practices for Users of Radioactive Sources,” ORS, Washington, DC, (2018).
[11] IAEA, “Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain,” IAEA, Vienna, (TBD).
[12] ISO/IEC, “Information Technology – Security Techniques – Information Security for Supplier Relationships – Parts 1 through 4” ISO/IEC 27036, ISO/IEC, Geneva, (2013-6)
[13] ISO/IEC, “Information technology — Security techniques — Information security risk management” ISO/IEC 27005:2018, ISO/IEC, Geneva, (2018).
[14] ISO/IEC, “Information technology — Security techniques — Information security management systems — Overview and vocabulary” ISO/IEC 27000:2018, ISO/IEC, Geneva (2018).
[15] IAEA, “Computer Security for Nuclear Security” Nuclear Security Series No. 42-G, IAEA, Vienna, (2021).
[16] INL, “Deconstructing the Nuclear Supply Chain Cyber-Attack Surface”, INL/CON-20-58484-Revision-1, INL, Idaho Falls, (2020).
[17] M. Jankowicz and C. Davis, “These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia,” 14 December 2020. [Online]. Available: https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12.
[18] FIREEYE, “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor,” 13 December 2020. [Online]. Available: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.
[19] L. Constantin, “SolarWinds attack explained: And why it was so hard to detect,” 15 December 2020. [Online]. Available: https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.
[20] Mimecast, “Incident Report,” 16 March 2021. [Online]. Available: https://www.mimecast.com/incident-report/.
[21] Elekta, “Elekta,” [Online]. Available: https://www.elekta.com/company/. [Accessed 23 February 2022].
[22] J. Davis, “Ransomware: Extortion Actors Leak Data, Vendor Attack Disrupts Services,” 2021 April 2021. [Online]. Available: https://healthitsecurity.com/news/ransomware-extortion-actors-leak-data-vendor-attack-disrupts-services.