

# The Anatomy of ICT and Services Supply Chain Risk Management

Innovative cyberattacks are emerging across the world in the wake of the COVID-19 pandemic. Attackers are using more sophisticated tools, techniques and processes (TTPs), including information and communications technology (ICT) and services supply chains, as increasingly effective channels for launching cyberattacks. The SolarWinds attack, which targeted hundreds of organizations through ICT supply chains, opened a Pandora's box of hidden risk and created panic waves among global IT and security leaders.<sup>1</sup> Apart from product-based industries, many enterprises do not instruct their risk management teams to cover ICT supply chains, even though most often do have risk management controls implemented for their ICT services chains. Cyberattacks target ICT and services supply chains in every type of business, including service-driven ones; therefore, ICT and services supply chain risk management should be a critical part of an organization's enterprise risk management framework.

## What Is the ICT and Services Supply Chain?

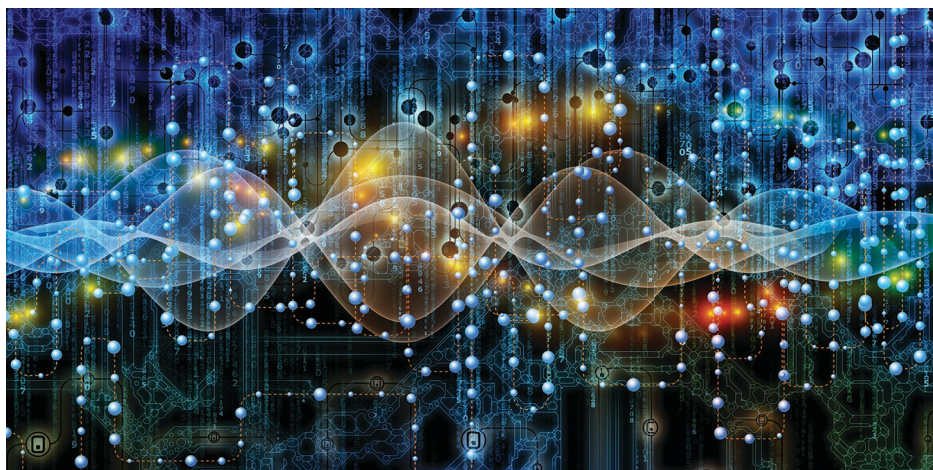
The ICT and services supply chain is the entire chain of activities connecting the life cycle of procurement and maintenance of ICT systems and services. More specifically, the ICT supply chain is an ecosystem that covers the entire life cycle of ICT hardware and software provided by third-party vendors, suppliers, system integrators and contractors and a wide range of managed services by various providers. Globally, enterprises depend on various suppliers for acquiring and maintaining new ICT systems and equipment. Servers, endpoints, network devices, software, electrical and electronic components, and a variety of services are procured from suppliers across the globe that may have their own internal suppliers. The SolarWinds attack leveraged the vulnerability that existed in the supply chain of the SolarWinds Orion business software.<sup>2</sup> In response, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an

emergency directive to mitigate and prevent against the SolarWinds compromise.<sup>3</sup> Furthermore, the US Government Accountability Office (GAO) issued a report in December 2020 that mandates enterprises take quick action to mitigate the risk that exists in their ICT and services supply chains.<sup>4</sup>

## Hidden Risk in ICT and Services Supply Chains

Several key risk factors need to be investigated for ICT and services supply chains to establish appropriate risk mitigation controls:

- Delivery of vulnerable software into the supply chains
- Software upgrades infected with malware



### Vimal Mani, CISA, CISM, Six Sigma Black Belt

Is the head of the information security department at the Bank of Sharjah. He is responsible for the bank's end-to-end cybersecurity program, coordinating cybersecurity efforts within the banking operations spread across the Middle East. Mani is also responsible for coordinating bank-wide cybersecurity strategy and standards, leading periodic security risk assessment efforts, leading incident investigations and resolution, and coordinating the bank's security awareness and training programs. He is an active member of the ISACA® Dubai (United Arab Emirates) Chapter. He can be reached at [vimal.consultant@gmail.com](mailto:vimal.consultant@gmail.com).

- Counterfeit devices and components
- Unsecured production infrastructure
- Ineffective contracts signed with suppliers

### Mitigating the Risk of Introducing Vulnerable Software Into Supply Chains

Enterprises use a variety of software development life cycle (SDLC) models, such as the Waterfall Model, Rational Unified Process (RUP), Spiral Model, Agile Methods, Capability Maturity Model Integration (CMMI) and DevOps. Most of these models lack secure software development practices, which results in vulnerable software. To overcome this risk, enterprises should consider incorporating security controls across their SDLC or use exclusive secured SDLC models,<sup>5</sup> such as the Building Security in Maturity Model (BSIMM), Software Assurance Maturity Model (SAMM), the Microsoft Security Development Lifecycle (SDL) or the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27034 standard.

“**SECURE SOFTWARE DEVELOPMENT MODELS CAN HELP CREATE SECURE AND RESILIENT SOFTWARE APPLICATIONS THAT KEEP OUT HACKERS.**”

Writing secure code is critical to ensuring the reliability and resiliency of software. Most weaknesses are found in the design or implementation phases of the SDLC. Hackers are smart and well versed in software development; therefore, it is critical to have a thorough understanding of how software can be exploited to effectively protect it and the data it processes. Secure software development models can help create secure and resilient software applications that keep out hackers. Those include:

- **BSIMM**—A study of existing software security initiatives observed in more than 100 organizations worldwide. As new development methodologies and threats emerge, the BSIMM will evolve.<sup>6</sup>

- **SAMM**—A framework that helps organizations develop, implement and improve their software security postures in a measurable manner. SAMM is based on 12 security practices grouped into five business functions. Every security practice can be further elaborated into a set of activities. Developed by the Open Web Application Security Project (OWASP), SAMM helps organizations improve their software security postures by integrating various security controls into their existing SDLCs.<sup>7</sup>
- **Microsoft SDL**—A result of Microsoft Corporation's Trustworthy Computing initiative for ensuring that its product development teams are developing secure, available and reliable software.<sup>8</sup>
- **ISO/IEC 27034 Information technology—Security techniques—Application security**—Provides guidance for integrating security controls across the application development life cycle. These guidelines are applicable for in-house and outsourced application development ecosystems. They provide a process framework for ensuring that sensitive applications developed by financial services, healthcare, defense, aviation, medical device manufacturing and mission-critical industries meet security expectations before software-oriented products hit the market. Application security control (ASC) is the most critical element of ISO/IEC 27034 because it helps strengthen security in applications.<sup>9</sup>

### Software Security Improves User Experience

Software security, safety and reliability are the core elements of software usability. Reviewing software usability from the end-user perspective involves critical elements such as how easy the product is to use, how secure the product is from hackers and how reliable the software operates after deployment. Considerations for mission-critical software used in aircraft, defense systems and implantable medical devices and software used by critical infrastructures such as nuclear power plants, airports, dams and refineries, include how safe the software is to use—the failure of which should not impact human lives. Therefore, in addition to having an uncomplicated graphical user interface (GUI), strengthening the security, reliability and safety aspects of software results in a more optimized end-user experience.

## Mitigating the Risk of Infectious Software Upgrades

In the SolarWinds attack, a trojan back door named SUNBURST<sup>10</sup> was inserted into the Orion software platform upgrade, which could have been prevented had the organizations that used the SolarWinds Orion platform implemented robust ICT and services supply chain risk management controls, such as deployment planning, rollback strategy planning, vulnerability scanning, security risk assessment and penetration testing in a test environment—critical activities to perform before deploying upgrades in production environments. Production deployment techniques such as testing using limited deployments; deployment using parallel environments; deployment of frequent, small and reversible changes; fully automated integration and deployment environments; and fully automated testing and rollback should be appropriately implemented. This helps ensure that an upgrade is stable in performance and no vulnerabilities exist that might be exploited later. Appropriate product/security documentation supporting any upgrades must be reviewed thoroughly to ensure that all critical activities are completed before deploying the upgrade in production environments. In addition, the product teams need to ensure that their products are phased in and phased out appropriately with well-defined product road maps. Having products that are not upgraded or patched can lead to security compromises in ICT supply chains.

## Mitigating the Risk of Counterfeit Devices and Components

Counterfeit products are products that are a copy or substitute of existing industry standard products without legal rights or authority and are misrepresented by the supplier. Counterfeit software and hardware products can be used as vehicles for Trojan malware such as the SUNBURST malware identified in the SolarWinds Orion upgrade, and can compromise the entire IT Infrastructure of the organization, which could lead to significant business disruption and losses. Counterfeit products are sold on black markets, which is a significant risk in ICT supply chain. When devices and components are bought from a source other than the original equipment manufacturer (OEM) partners or other authorized sources, the source

“ DUE TO THE INEFFECTIVE SECURITY POSTURE OF PRODUCTION ENVIRONMENTS, THERE ARE OPPORTUNITIES FOR VULNERABLE SOLUTIONS AND PRODUCTS TO BE DEVELOPED AND SUPPLIED TO CLIENTS. ”

should be closely reviewed if it is unknown, is from a troubled geopolitical location, has set a suspiciously low price, or is being too flexible or agreeable. Products are counterfeit when the cost of the original, genuine components is more in the market cost. Availability shortages of original equipment can also lead to the emergence of these counterfeit products. Counterfeit Parts Standards such as AS5553, AS6081, AS6171, AS6496, and DFARS: 252.246.7007 need to be considered appropriately in the procurement life cycle of counterfeit products.<sup>11</sup> Having controls implemented will help prevent organizations from the risk of buying and using counterfeit products in their organizations, including:

- Visual inspections of the products
- Destructive and nondestructive tests conducted for the products
- Product safety and security assurance review by third party
- Review of product manuals
- On-site supplier audits
- Implementation of a material control and reporting process
- Implementation of a well-defined vendor management process framework
- Implementation of periodic vendor risk assessments

## Mitigating the Risk of Unsecured Production Infrastructure

Due to the ineffective security posture of production environments, there are opportunities for vulnerable solutions and products to be developed and supplied to clients through their existing ICT supply chains. Risk management controls need to be planned and implemented to protect the production environments, such as:

- A variety of cybersecurity controls needs to be planned and implemented in a relevant manner by considering the production environments.
- Suitable security controls need to be implemented across the software supply chain to protect products from security compromises.
- Periodic cybersecurity risk assessments targeting production environments need to be planned and executed.
- The integrity of the finished products needs to be assured before moving to the ICT supply chains, with confirmation that products with approved configurations are shipped and products are not compromised by malware that can be exploited by hackers.
- How a technology refresh related to a product will be managed (upgrades and patches)
- Terms and conditions related to product support
- How a product life cycle will be managed (phasing out end-of-life products and phasing in new products)
- Terms and conditions related to information and cybersecurity posture of the products and the details of various assessments carried out. This will increase confidence in the security and reliability of the products moving across the supply chain.
- Terms and conditions related to intellectual property rights management and breach-related repercussions
- Right to audit the suppliers as needed
- Reference on conducting periodic contract reviews

“ THE PERFORMANCE OF THE SUPPLY CHAIN AND STRENGTH OF SUPPLY CHAIN RISK MANAGEMENT CONTROLS NEED TO BE BENCHMARKED IN PERIODIC INTERVALS BY THE ORGANIZATION. ”

### Mitigating the Risk of Ineffective Contracts Signed With Suppliers

Most contracts signed with suppliers only address factors such as price, service and warranty schemes in a larger context. These contracts generally lack terms and conditions related to cybersecurity assurance regarding the products/services moved into the ICT and services supply chain. Product vendors releasing their products into global ICT and services supply chains should ensure that there is an adequate amount of clarity on specific points in their signed contracts. Those include:

- Security methodologies/guidelines adopted in the development life cycle
- Security methodologies/guidelines to be adopted during product implementation

Conducting periodic contract reviews of suppliers involved in the ICT and services supply chain helps organizations proactively identify gaps and vulnerabilities in their products and services in a timely manner so they can plan the remediation actions required to sustain and improve the experience of their customers.

### Strengthening the Maturity of ICT and Services Acquisition Infrastructure

Organizations should plan to implement best practices such as the US National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*<sup>12</sup> and ISO/IEC 12207<sup>13</sup> to secure their ICT products and services acquisition life cycle and address the potential risk. The acquirer of ICT products and services must ensure that they have assurance from their suppliers that adequate information security and risk management controls have been implemented on the supplier's end. Based on capability maturity models such as the Software Acquisition Capability Maturity Model (SA-CMM),<sup>14</sup> the performance of the supply chain and strength of supply chain risk management controls need to be benchmarked in periodic intervals by the organization. The SA-CMM



helps the organization identify improvements in key process areas of the ICT and services supply chain and mitigate the critical risk to which it is exposed.

### Defined Vendor Management Practices

It is critical for organizations acquiring ICT products and services to have a well-defined vendor management framework in place to help select appropriate vendors and maintain low-risk relationships throughout the contract life cycle. This vendor management framework should cover critical aspects of vendor life cycle stages such as vendor selection, contracting, contract change management, contract renewal, onboarding of vendors, vendor performance management, vendor transition and vendor risk management. **Figure 1** illustrates the vendor management types of risk faced by global organizations.

### Key Risk Indicators for Effective Vendor Risk Management

There are sample key risk indicators (KRIs) that should be tracked in a timely manner to help the organization address critical vendor management risk, including:

- Increasing dependency on specific vendor(s)
- Having the same vendor involved in multiple projects on an ongoing basis
- Increasing the cycle time for delivery of services and products

- Increasing the amount of quality and security issues found in services and products delivered by the vendor(s)
- Seeing an increasing trend in prices quoted by vendors
- Seeing an increasing amount of security issues found with vendor staff deployed onsite
- Seeing an increasing amount of security issues found in audits performed with vendor facilities

### Categorization of Vendor Risk and Mitigation Strategies

Not all vendor risk is the same and the risk often needs to be mitigated using different strategies. The risk profile of an organization's vendors should be assessed, and suitable risk mitigation strategies need to be identified and implemented. **Figure 2** illustrates risk profile vs. mitigation strategy mapping.

### Improving Vendor Risk Management Practice

The maturity of vendor risk management practice can be improved by implementing the right set of cybersecurity, IT, privacy, data security and business resilience controls. Vendor risk management practices need to be benchmarked on a regular basis against appropriate maturity models available in the market, such as the Vendor Risk Management Maturity Model (VRMMM),<sup>15</sup> which helps organizations identify specific areas for improvement

**Figure 1—Vendor Management Risk**

Type of Risk	Description of Risk Events
Security and privacy risk	Risk from data breaches and leakages
Compliance risk	Risk related to laws and regulations
Reputation risk	Law violations, dissatisfied customers
Operational risk	Risk triggered by people, processes, systems and external events
Transaction risk	Service delivery failure
Credit risk	Vendors not able to meet contract payment-related terms and conditions
Legal risk	Risk triggered by vendors' inability to enforce contractual terms due to legal jurisdiction
Country risk	Risk from geopolitical, economic and social issues
Business continuity risk	Risk from having a lack of adequate disaster recovery and business continuity plans for critical business processes
ICT supply chain risk	Intentional insertion of malicious functionality into the software acquired, supply of counterfeit components, poor programming, poor quality and poor performance of products

### Enjoying this article?

- Read *EU Financial Sector Digital Operational Resilience: A Risk Approach*. [www.isaca.org/eu-financial-sector-operational-resilience](http://www.isaca.org/eu-financial-sector-operational-resilience)
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>



Figure 2—Vendor Risk Mitigation		
Vendor Risk Profile	Risk Exposure	Risk Mitigation Strategy
High risk	Potential revenue loss is possible.	1. Start identifying new vendors. 2. Consult legal counsel for making claims for any revenue losses incurred due to the vendor.
Medium risk	Quality and reliability issues are found in an overwhelming manner in the service/ product delivered by the vendor.	1. Track KRIs in a timely manner and take corrective measures. 2. Conduct vendor reviews on a regular basis to discuss the issues found.
Low risk	Minor issues are found in the service/ product delivered by the vendor.	1. Continuously monitor until seeing a downward trend in the KRIs. 2. Continue enforcing the service level agreement terms and conditions agreed on with the vendor.

and make well-informed decisions that drive efficient resource allocation and use, and help manage vendor management-related risk effectively.

By evaluating the level of maturity for each component (or subcomponent) of the model, the VRMMM incorporates vendor risk management best practices into a usable model that can be used to assess the current and desired future state of an organization's vendor risk management program. Maturity levels for each component of the VRMMM cover the entire spectrum of possibilities, ranging from nonexistent to continuous improvement.

**“TO HAVE A RISK-CONTROLLED ICT AND SERVICES SUPPLY CHAIN, ENTERPRISES SHOULD CONSIDER HAVING A STRONG AND SECURED ACQUISITION INFRASTRUCTURE.”**

## Conclusion


The SolarWinds attack demonstrated that the vulnerabilities present in ICT and services supply chains can be successfully exploited by hackers. The vulnerabilities that exist in the ICT and services supply chain, either intentionally or unintentionally, can result in serious compromises such as exploitation, leading to system and network failures. To have a risk-controlled ICT and services supply chain, enterprises should consider having a strong and secured acquisition infrastructure, vendor management practices, robust controls, and

assessments addressing potential issues related to product safety, security and reliability. Enterprises should also conduct periodic benchmarking and maturity reviews of their supply chain and their supply chain partners, whose inputs can help the enterprise increase the end-user experience for their ICT products and services. In addition, enterprises should assess the trustworthiness of their global ICT supply chains by having independent ICT and services supply chain assurance audits carried out by third-party auditors and subject-matter experts.<sup>16</sup>

## Endnotes

- 1 Tung, L.; “SolarWinds Attack Hit 100 Companies and Took Months of Planning, Says White House,” ZDNet, 18 February 2021, <https://www.zdnet.com/article/solarwinds-attack-hit-100-companies-and-took-months-of-planning-says-white-house/>
- 2 FireEye, “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor,” 13 December 2020, <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>
- 3 US Cybersecurity and Infrastructure Security Agency, “Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise,” USA, 13 December 2020, <https://cyber.dhs.gov/ed/21-01/>
- 4 United States Government Accountability Office (GAO), *Report to Congressional Requesters: Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, USA, December 2020, <https://www.gao.gov/assets/gao-21-171.pdf>

- 5 HackEDU, "What Is a Secure Software Development Lifecycle and How Do You Build an Appsec Program?" <https://www.hackedu.com/blog/what-is-a-secure-software-development-lifecycle-and-how-do-you-build-an-application-security-program>
- 6 Building Security In Maturity Model (BSIMM), "About the BSIMM," <https://www.bsimm.com/about.html>
- 7 Open Web Application Security Project (OWASP), "Software Assurance Maturity Model," <https://owaspsamm.org/>
- 8 Microsoft, "About Microsoft SDL," <https://www.microsoft.com/en-us/securityengineering/sdl/about>
- 9 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27034:2011 *Information Technology—Security Techniques—Application Security*, Switzerland, 2011, <https://www.iso.org/standard/44378.html>
- 10 Malwarebytes Labs, "Backdoor.Sunburst," <https://blog.malwarebytes.com/detections/backdoor-sunburst/>
- 11 Bodemuller, B.; *Counterfeit Prevention: Past, Present and Future*, Lockheed Martin, USA, 2020, <https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/suppliers/training-2020-counterfeit-parts.pdf>
- 12 National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, USA, April 2015, <https://csrc.nist.gov/publications/detail/sp/800-161/final>
- 13 Institute of Electrical and Electronics Engineers (IEEE), *IEEE 12207-2-2020 - ISO/IEC/IEEE International Standard - Systems and software engineering—Software life cycle processes—Part 2: Relation and mapping between ISO/IEC/IEEE 12207:2017 and ISO/IEC 12207:2008*, USA, 23 October 2020, <https://standards.ieee.org/standard/12207-2-2020.html>
- 14 Software Engineering Institute, *Software Acquisition Capability Maturity Model (SA-CMM) Version 1.03*, 2002, <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6099>
- 15 Shared Assessments, *Vendor Risk Management Maturity Model (VRMMM)*, <https://sharedassessments.org/vrmmm/>
- 16 Zazakova, A.; "Assessing the Trustworthiness of ICT Supply Chains: Why and How?" Kaspersky, 2 April 2020, <https://www.kaspersky.com/about/policy-blog/general-cybersecurity/assessing-the-trustworthiness-of-ict-supply-chains-why-and-how>



**ONE IN TECH™**  
An ISACA Foundation

Join ISACA's Foundation in building the current and future **Digital Trust workforce** by fostering a **diverse and inclusive** pipeline of professionals.

[www.oneintech.org](http://www.oneintech.org)