SECURING SMALL AND MEDIUM-SIZED BUSINESS SUPPLY CHAINS

A resource handbook to reduce information and communication technology risks

OVERVIEW

DISCLAIMER

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this report or otherwise. This report is TLP: CLEAR: Disclosure is not limited. Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see www.cisa.gov/tlp.

Supply chain information and communications technology (ICT) related risks are increasing nationwide. They are potentially more harmful to small and medium-sized businesses (SMBs), especially compared to larger entities. Data from the U.S. Small Business Administration shows SMB information technology (IT) and communications providers represent more than 160,000 companies in the United States; connect millions of households and businesses to the internet every day; and acquire, build, and integrate technology solutions for themselves and their customers[1]. Implementing supply chain security practices is therefore critical for these ICT entities.

For many, knowing where to start—and how an SMB can take on the financial, personnel, or other resources necessary to implement certain ICT supply chain practices—can seem overwhelming. As a result, the ICT Supply Chain Risk Management (SCRM) Task Force SMB Working Group (WG), was tasked with identifying ICT-related supply chain risks that an IT and communications SMB might encounter with a focus on cyber risks and how those risks might be different than in larger companies (hereinafter referred to as "ICT supply chain risk(s)").

The WG used a variety of approaches and techniques to gain insight into the highest ICT supply chain risk categories commonly faced by IT and communications SMBs. Part of that process included a focus-group made

[1] Source: Office of Advocacy, U.S. Small Business Administration from data provided by the U.S. Census Bureau, Statistics of U.S. Businesses.

up of communications SMBs, conversations with various industry groups, government agencies, and subject matter experts. The WG also received feedback from approximately 100 IT SMBs, 64 percent of whom had 100 or fewer employees.

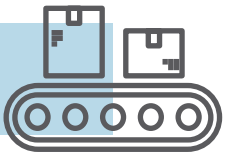
More than a dozen ICT supply chain risk categories were initially identified. Following further scoping and refinement, the following six categories emerged as the highest priority ICT supply chain risk categories for IT and communications SMBs.

ICT SUPPLY CHAIN RISK CATEGORIES

1//CYBER EXPERTISE
2//EXECUTIVE COMMITMENT
3//ICT SUPPLY CHAIN RISK MANAGEMENT
4//SINGLE SOURCE SUPPLIER
5//SUPPLIER DISRUPTION
6//SUPPLIER VISIBILITY

Recognizing that many IT and communications SMBs do not have dedicated risk management experts or functions internally, the WG prepared this resource handbook. This handbook includes six use cases to help these SMBs recognize common ICT supply chain risk challenges as well as provides practical and actionable measures they can take to mitigate these risks. The use cases are based on fictional ICT companies and present scenarios that these SMBs may face. They also highlight one or more of the six risk categories, propose potential options that the fictional company may consider, provide a short summary of costs and benefits associated with implementing the proposed options, and provide a section of government and industry mitigation resources that can be accessed for more detail.

While the target audience for the resource handbook is IT and communications SMBs, the categories, use cases, and suggested resources are relevant to SMBs of all industries.



KEY SMB ICT SUPPLY CHAIN RISK CATEGORIES

1//CYBER EXPERTISE

Description: The availability of knowledge, skills, and experience necessary to establish, implement, and manage ICT SCRM practices. Collaborating is a key factor for a company to invest in cyber expertise most effectively.

Recommended mitigation resources for this risk category:

CISA: CISA Cyber Essentials
CISA: Cyber Resilience Review Assessment
CISA: Cyber Security Evaluation Tool (CSET®)
NIST: Ransomware Resources
NIST: NIST Cybersecurity Framwork (CSF) Quick Start Guide
NIST: Small Business Cybersecurity Corner (including Cybersecurity Case Study Series)

2//EXECUTIVE COMMITMENT

Description: Company leadership, knowledge and understanding of cybersecurity as a business risk and a willingness to foster an organization-wide cyber risk awareness culture, prioritize cybersecurity risk management, and enable secure supply chain practices necessary to protect the company, its assets, employees, and customers.

Recommended mitigation resources for this risk category:

CISA: CISA Cyber Essentials
CISA: Cyber Guidance for Small Businesses
DNI: Supply Chain Best Practices
GCA: Cyber Basics for Small Businesses Training
NIST: Baldrige Cybersecurity Excellence Builder
NIST: NIST Small Business Cybersecurity Corner

3//ICT SUPPLY CHAIN RISK MANAGEMENT

Description: Processes and practices ensuring the integrity of your supply chain aimed at improving a company's cybersecurity practices by identifying, assessing, and mitigating the risks associated with information technology products and services. This can include engaging relevant stakeholders, investing in the appropriate resources to protect the company's data, and integrating cybersecurity practices into the company's decision making, budget, and operational processes.

Recommended mitigation resources for this risk category:

CISA: ICT Supply Chain Risk Management Fact Sheet
CISA: Internet of Things (IoT) Acquisition Guidance
CISA: Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses
CISA: Best Practices in Cyber Supply Chain Risk Management
CISA: CISA Cyber Essentials
CISA: Cyber Resilience Review Assessment
CISA: Cyber Security Evaluation Tool (CSET®)
FEDVTE: Cyber Supply Chain Risk Management for the Public
NCSC: Framework for Assessing Risks
NCSC: Supply Chain Best Practices
NIST: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
NIST: NISTIR 83ware Risk Management: A Cybersecurity Framework Profile | CSRC
NIST: Risk Management Framework for Systems and Organizations Introductory Course
NIST: Small Business Cybersecurity Corner
NIST: Ransomware Resources
NIST: NIST CSF Quick Start Guide

4//SINGLE SOURCE SUPPLIER

Description: Suppliers who are preferred for a particular product or service or are a sole supplier of a given product or service.

Recommended mitigation resources for this risk category:

CISA: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses

5//SUPPLIER DISRUPTION

Description: Any attempt to degrade an ICT provider's supply chain with the intent to disrupt ongoing operations, damage, or breach data contained on the system or network.

Recommended mitigation resources for this risk category:

CISA: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services
CISA: Cybersecurity Incident and Vulnerability Response Playbooks
ENISA: Threat Landscape for Supply Chain Attacks — ENISA (europa.eu)

6//SUPPLIER VISIBILITY

Description: The need for visibility into third-party cybersecurity practices.

Recommended mitigation resources for this risk category:

CISA: Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses

CISA: Internet of Things (IoT) Acquisition Guidance
NASA: NASA SEWP Certified Vendors
NIST: Executive Order (EO) Guidance for Cybersecurity Supply Chain Risk Management
NIST: NIST Secure Engineering

NIST: Software Security in Supply Chains: Enhanced Vendor Risk Assessments
NTIA: Roles and Benefits for SBOM Across the Supply Chain
NTIA: Software Bill of Materials Resources

USE CASES

	page number	5	6	7	8	10	12
	ICT SUPPLY CHAIN RISK CATEGORIES / **USE CASES**	**Rural Utility Services (RUS):** Broadband Service Provider	**Micro Coding Wizards (MCW):** Software Company	**Cloud Information Systems (CIS):** IT Company	**GreyCo:** US Defense Integrator	**SubZeroQ:** Quantum Computing	**AIO Company:** ICT Provider
1	CYBER EXPERTISE						●
2	EXECUTIVE COMMITMENT			●	●		●
3	ICT SUPPLY CHAIN RISK MANAGEMENT	●	●	●	●		●
4	SINGLE SOURCE SUPPLIER					●	●
5	SUPPLIER DISRUPTION			●			●
6	SUPPLIER VISIBILITY	●	●		●		●

USE CASE SCENARIO:
RURAL UTILITY SERVICES (RUS)

RUS is a small broadband service provider with a broadband network servicing 5,000 customers. RUS management has identified a need to implement an outage management system (OMS) that is used to track customer outages, as well as other types of outages (i.e., broadband fiber lines and equipment). RUS issued a request for proposal (RFP) for this new OMS and an award was issued to a small IT software development company, Micro Software Wizards (MSW), to develop, support and maintain the OMS software over a 5-year period.

A contract was signed between RUS and MSW which included the following ICT-SCRM contract provisions:

- MSW must supply RUS with software supply chain attestations showing software development life cycle (SDLC) and cybersecurity practices, along with attestations acknowledging MSW's adherence to cybersecurity and SDLC policies and practices, following National Institute of Standards and Technology (NIST) recommendations.
- MSW must notify RUS of any newly discovered vulnerabilities affecting the OMS software within 24 hours of first discovery.
- RUS must provide MSW with secure, remote, multi-factor authentication virtual private network access to perform customer support activities.

ICT SUPPLY CHAIN RISK CATEGORIES

3//ICT SUPPLY CHAIN RISK MANAGEMENT
RUS does not have an internal ICT SCRM program or dedicated risk management staff and lacks a structure or framework to effectively identify, assess, and mitigate risks that MSW's OMS software may present.

6//SUPPLIER VISIBILITY
RUS lacks access to MSW's processes or practices to fully understand MSW's cybersecurity posture.

POTENTIAL OPTIONS FOR RUS

Consider engaging a third-party ICT SCRM consultant to use a proven risk management framework to help RUS identify, asses, and mitigate actual or potential risks from MSW's OMS software.

Modify MSW's contract to require that they complete the Vendor SCRM Template for SMBs.

COST AND BENEFITS

POTENTIAL COSTS
Independent consultant hourly rates can range from $75/hr - $250/hr

POTENTIAL BENEFITS
Access to ICT SCRM expertise on an as needed basis versus the costs of a full-time internal hire.

Visibility into, and better understanding of, MSW's SDLC and cybersecurity practices provides stronger confidence.

RESOURCES

CISA: Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses
CISA: Best Practices in Cyber Supply Chain Risk Management
CISA: Internet of Things (IoT) Acquisition Guidance
FEDVTE: Cyber Supply Chain Risk Management for the Public
NIST: Risk Management Framework for Systems and Organizations Introductory Course

USE CASE SCENARIO:
MICRO CODING WIZARDS (MCW)

MCW is a small software development company providing software solutions to help manage a fleet of electric vehicles for corporations. MCW's software solution, MCWManager, is an asset management platform specifically designed to manage electric vehicle fleets. MCWManager tracks usage, charge level, range, and other important characteristics of each electric vehicle in the fleet. The U.S. Department of the Interior (DOI) has expressed interest in licensing the MCWManager software to manage a fleet of 20 electric vehicles, spread across the Western Region, which includes states west of the Rocky Mountains. MCW has been informed by the DOI that their software will need to supply a software bill of materials (SBOM) as well as a vulnerability disclosure report attestation to the DOI prior to procurement. MCW's current software development life cycle process lacks an ICT SCRM capability, which hinders MCW's production of a SBOM and a vulnerability disclosure report.

ICT SUPPLY CHAIN RISK CATEGORIES

3//ICT SUPPLY CHAIN RISK MANAGEMENT
MCW lacks an ICT SCRM process and is not currently producing a SBOM or vulnerability disclosure report documents in their build process. Change is needed to MCW's build process to produce these documents.

6//SUPPLIER VISIBILITY
The DOI is following NIST software supply chain recommendations for software vendors to provide attestations of processes and procedures in MCW's software development life cycle. This information will give the DOI greater visibility into MCW's software components and any vulnerabilities that may present in the MCWManager application, prior to purchasing the product.

POTENTIAL OPTIONS FOR MCW

Follow NIST recommendations to generate a SBOM and a vulnerability disclosure report for MCWManager.

Integrate a SBOM and a vulnerability disclosure report into the development operations (DevOps) Build Process, using an open-source SBOM and vulnerability disclosure report tools.

Provide customers with secure access to the MCWManager SBOM and vulnerability disclosure report attestations.

COST AND BENEFITS

POTENTIAL COSTS
Time and effort of build engineers to implement free, open-source tools to produce a SBOM and a vulnerability disclosure report during the build process.

POTENTIAL BENEFITS
Satisfy DOI requirements, positioning MCW to secure a potential government contract for the MCWManager application.

MCW gains visibility into their own software supply chain of components providers and open-source software.

Visibility into and better understanding of MSW's SDLC and cybersecurity practices, providing stronger confidence in the security of MSW's products.

RESOURCES

CISA: ICT Supply Chain Risk Management Fact Sheet
CISA: Supply Chain Risk Management- YouTube
NIST: EO Guidance for Cybersecurity Supply Chain Risk Management
NIST: NIST CSF Quick Start Guide
NTIA: Software Bill of Materials Resources

USE CASE SCENARIO: **CLOUD INFORMATION SYSTEMS (CIS)**

CIS is an IT firm operating a software as a service customer billing service called CISCustomerManager (CCM) to rural broadband operators. CIS provides customer billing services for 230 broadband operators across the United States, servicing 420,000 broadband customers with an average bill of $60/month for a total monthly billing revenue of $25,200,000. CIS has eight employees with monthly revenues of $2,300,000. CCM operates in the cloud using a web-based front-end to interact with CCM customers in the broadband community. In March of 2019, the IT Director for CIS approached the Chief Executive Officer (CEO) with a proposal to implement an incident response plan that required investment in a business continuity plan (BCP) to enable CIS to quickly recover from a debilitating cybersecurity incident, such as a ransomware attack that would encrypt CIS's data and applications, essentially disabling CIS's ability to operate its CCM application. The BCP proposal had an estimated one-time cost of $100,000 and $25,000 annually and would enable CIS to recover full production operations of the CCM platform within four hours. After initial consideration, the CEO rejected the proposal and CIS continued operating without a BCP in place. In January 2022, CIS was attacked using the Log4j vulnerability, resulting in a ransomware attack that disabled CIS from billing customers for four months and cost CIS $500,000 in recovery expenses. This significantly impacted cash-flow and impacted all 230 CIS customers' billing operations.

ICT SUPPLY CHAIN RISK CATEGORIES

2//EXECUTIVE COMMITMENT
AND
5//SUPPLIER DISRUPTION

The CEO of CIS rejected a $100,000 proposal to implement a BCP using a hot backup site that could have allowed CIS to recover from a ransomware attack in four hours. CIS was unable to bill customers for four months resulting in significant cash-flow shortages, leading to expensive loans to keep operations running. CIS customers were also unable to bill their own customers for four months, totaling more than $100,000,000 in broadband customer bills.

3//ICT SUPPLY CHAIN RISK MANAGEMENT

The CCM cloud platform was out of operation for four months due to poor cyber hygiene that failed to patch the Log4j vulnerability in a timely manner.

POTENTIAL OPTIONS FOR CIS

Spend the $100,000 to implement the BCP to reduce recovery time in the future.

Immediately patch the Log4j vulnerability to prevent a successful attack leveraging this vulnerability.

Operate a "hot backup" of the CCM application on another cloud platform that remains in "standby mode" until called into service.

COST AND BENEFITS

POTENTIAL COSTS

$100,000 to implement a BCP using a digital twin and $25,000 annually to maintain the service. One full time engineer to manage the digital twin environment.

POTENTIAL BENEFITS

Four hour recovery time versus being out of service for four months and unable to send bills to customers.

No loss of cash-flow for four months for CIS and its 230 broadband customers.

RESOURCES

CISA: CISA Cyber Essentials
CISA: Cyber Guidance for Small Businesses
CISA: Cybersecurity Incident and Vulnerability Response Playbooks
ENISA: Threat Landscape for Supply Chain Attacks — ENISA (europa.eu)
NIST: NIST CSF Quick Start Guide

USE CASE SCENARIO: **GREYCO**

GreyCo is a medium-sized U.S. defense integrator providing customized systems and solutions. GreyCo provides a unique field hardened solution for collecting radio signal interception, collection, and decoding. GreyCo has extensive expertise and intellectual property in radio signal interception and decoding. The majority of their product is sourced from multiple vendors including a major systems manufacturer, standard integrated circuits (IC)s on which their software is burned and hosted, as well as several hundred commodity electronics parts. GreyCo has been sub-contracted by a prime contractor to provide an important element of a new major mobile platform contract awarded by the U.S. Army. The prime contractor has required GreyCo to provide evidence that they are sourcing from trusted sources and their integration practices mitigate the risk of counterfeit and tainted components. This evidence must be provided as a prerequisite for the award of the sub-contract. Additionally, GreyCo is required to provide evidence they are employing modern secure engineering practices in the process of manufacturing their solutions.

GreyCo has a history of compliance with federal cybersecurity standards; however, GreyCo does not have a significant background in supply chain security and how those risk mitigations differ from pure cyber controls. The GreyCo Chief Technology Officer (CTO) conducts research on appropriate standards and notices that many similar sized companies have successfully obtained certification for providing SCRM mitigations that provide

evidence of meeting many federal agencies' SCRM requirements. The CTO attends several industry SCRM events and talks with several of the vendors, where he learns that most of the companies have hired consultants to help provide a pre-assessment of their sourcing and manufacturing processes. The GreyCo executive team attends a review of the assessment conducted by a consultant and learns about the necessary lifecycle, secure engineering, and procurement practices necessary to mitigate supply chain risks. Some GreyCo executives are reluctant to invest in the lifecycle, secure engineering, and procurement practices—because they want empirical evidence that their investment would result in greater opportunity and product capabilities. GreyCo empowers a working group responsible for defining the business case, updating GreyCo's practices, documenting their product lifecycle, governance, and implementation oversight processes to ensure continuous improvement.

GreyCo's CTO also works with GreyCo's lead product manager to adopt tooling and practices needed to address the identified gaps in GreyCo's secure engineering and supply chain practices. To achieve these updates, the GreyCo team leverages federal guidelines on secure engineering practices and quantitative risk analysis standards. Several weeks later, the GreyCo team submits a scope of evaluation of their SCRM practices for assessment and certification by an accredited lab. After the lab conducts the assessment and validates the provided evidence, GreyCo is notified that they meet the conformance criteria. GreyCo provides the evaluation and findings to the prime contractor and the award of their sub-contract is upheld. GreyCo uses its documented product development lifecycle, secure engineering and supply chain procurement, and governance practices to continuously improve its risk posture as new supply chain security threats are communicated.

ICT SUPPLY CHAIN RISK CATEGORIES

2//EXECUTIVE COMMITMENT
GreyCo executives were skeptical of funding additional risk mitigations without better understanding the return on their investment. GreyCo's CEO wanted empirical evidence that an investment would not only protect their reputation but would also drive additional revenue to cover added costs.

3//ICT SUPPLY CHAIN RISK MANAGEMENT
MCW lacks an ICT SCRM process and is not currently producing a SBOM or vulnerability disclosure report documents in their build process. Change is needed to MCW's build process to produce these documents.

6//SUPPLIER VISIBILITY
GreyCo wants to expand its business and sell into additional space and defense sectors. GreyCo recognizes that current policies require suppliers to follow industry best standards and standards within their manufacturing and supply chain practices. The GreyCo team funds an independent assessment and industry certification that can be used to meet their contractual obligations and their visibility as a trustworthy supplier.

POTENTIAL OPTIONS FOR GREYCO

Use a formal quantitative risk management standard to better determine where to apply resources across the GreyCo manufacturing and sourcing supply chain to maximize future revenue opportunities while minimizing the risk to their reputation and customers.

Obtain third-party independent assessment and certification to determine SCRM gaps while using federal secure engineering guidance and leveraging industry best practice frameworks.

Implement enhanced supplier sourcing practices while optimizing their development and manufacturing governance and oversight processes.

Communicate GreyCo's certification to government procurement entities. Use the assets created by the constant evaluation as evidence for compliance and future bids.

RESOURCES

CISA: CISA Cyber Essentials
NASA: NASA SEWP Certified Vendors
NIST: NIST Secure Engineering
NIST: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

COST AND BENEFITS

POTENTIAL COSTS

GreyCo decided to hire a consultant to conduct an assessment to help document current practices and identify where changes may be required to mitigate SCRM risk. GreyCo found that some gaps in development warranted new secure development operations (SecDevOps) tools and required a better governance process for managing and scoring suppliers. GreyCo evaluated the return on investment provided by the suggested mitigations and implemented new tooling for managing their product lifecycle. This included additional automated vulnerability analysis of the code they produced, including the open-source software used in their product.

POTENTIAL BENEFITS

Satisfy federal government requirements for suppliers, which will lead to increased opportunity by being listed as a trusted supplier.

Adopting a formal quantitative risk framework helped GreyCo better explain how they were applying company resources to mitigate SCRM risk against the industry best practices.

USE CASE SCENARIO: **SUBZEROQ**

Several U.S. Research Labs are looking to expand research on the application of quantum computing. One component that is needed for building or maintaining quantum computers is cryogenic superconductive cabling. These cables, unlike their copper counterparts, are made from an exotic and proprietary mix of rare earth elements using proprietary manufacturing practices. Procurement teams at the U.S. Naval Research Lab (NRL) are leading the procurement process. NRL determines that there is clearly only one supplier that meets their requirements, SubZeroQ.

A sole source supplier presents NRL with a unique supply chain security challenge. While SubZeroQ has a superior reputation in the quantum computing community, the NRL procurement team is responsible for rating SubZeroQ's SCRM practices before placing them on the preferred provider list. Much of the work being conducted by NRL is considered sensitive and requires limited

procurement visibility. NRL is particularly interested in ensuring SubZeroQ can provide a continued supply of rare earth minerals, protect the procurement information provided by NRL, and ensure the delivery of an authentic product to their customers.

NRL procurement reaches out to SubZeroQ to obtain a face-to-face briefing of their SCRM practices. To facilitate this discussion, NRL procurement officials meet to review the Cybersecurity and Infrastructure Security Agency (CISA) Vendor SCRM Template to determine which questions can help seed and guide the discussion with SubZeroQ. NRL comes up with a list of questions which includes:

- Is the continued supply of rare earth minerals contingent on a single source?
- Will the gating materials be supplied from a Country of Particular Concern?
- Are NRL customers and procurement activities protected and supported by the integrity of the SubZeroQ procurement systems?
- Is there a process used by SubZeroQ for reporting product and supply chain security incidents?
- What is the process to ensure the integrity and authentication of transportation and delivery of SubZeroQ products to the intended customer?

SubZeroQ meets with NRL to discuss the list of questions and review their practices for protecting their customers across the supply chain. SubZeroQ explains that they have divided their supply of raw and rare materials between two well-known sources and are paying higher prices in some cases to avoid high-risk suppliers. They provide NRL with a view into their supplier scoring framework and how they manage similar requirements from sub-suppliers. SubZeroQ explains which standards they are following to guide their SCRM practices. SubZeroQ also provided an end-to-end review of how they protect the transportation of products from their plant in Japan to their global clientele. This included tamper-resistant packaging as well as authentication coding of packages which provides coded tracking of packages as they travel through the distribution chain.

ICT SUPPLY CHAIN RISK CATEGORIES

3//ICT SUPPLY CHAIN RISK MANAGEMENT AND
4//SINGLE SOURCE SUPPLIER

SubZeroQ is the sole parts supplier for the super conducting cabling used in quantum computers. NRL is looking to provide their research labs with the ability to procure their products. NRL seeks confirmation that SubZeroQ can properly protect their procurement data, ensure long term supply, and effectively mitigate SCRM risks preventing counterfeit or replacement parts being inserted during transportation.

POTENTIAL OPTIONS FOR SUBZEROQ

SubZeroQ is in the unique position of being a sole supplier for a highly sought component. This warrants SubZeroQ to take a more hands on approach to interacting with customers seeking to understand how they approach SCRM, protect their customer procurement data, and ensure the untampered delivery of the product to their customers.

SubZeroQ procurement systems are hosted in a cloud-based environment and use international standards guidance for implementation of cyber controls. SubZeroQ recogniz-es the need to provide a cross walk between the inter-national standards implemented and country

level standards applicable to customers outside their home country.

SubZeroQ has developed a comprehensive briefing package and has empowered members of their Chief Information Security Officer's (CISO) team to travel to customers to provide direct briefings and answer questions about their practices.

A sanitized version of the SubZeroQ supply chain risk management plan has been drafted as a leave behind for customers. This effectively protects sensitive SubZeroQ information while providing procurement teams with additional information.

SubZeroQ has implemented a well-documented Product Security Incident Response Team (PSIRT) that will respond to any potential product transportation or fulfillment incidents. Each customer is provided direct contact to the PSIRT team to respond to potential incidents.

COST AND BENEFITS

POTENTIAL COSTS

SubZeroQ has empowered their CISO team to travel to NRL to provide a supplier SCRM briefing. They have also invested in the cross walks between the international standards they employ and U.S. national standards. SubZeroQ has also invested in a PSIRT responsible for managing and mitigating risks during procurement and fulfillment as well as communicating important security incidents to customers.

POTENTIAL BENEFITS

Satisfy federal government requirements for contracts, provide visibility into single source SCRM practices to obtain a preferred provider designation by U.S. agencies and companies.

RESOURCES

CISA: Internet of Things (IoT) Acquisition Guidance
NCSC: Framework for Assessing Risks

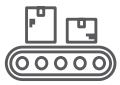
Risk Management Frameworks:
NIST: NIST Risk Management Framework

USE CASE SCENARIO: **AIO COMPANY (AIO)**

AIO is a mid-size organization with 100 employees located in various locations around the country. AIO is searching for ways to effectively communicate with their customers, as traditional telephone lines are no longer the primary contact route. After conducting research on several products, AIO identifies a product that offers voice, text, and live chat with screen sharing capabilities, filling all of the organization's customer service needs. The company's CISO is asked to perform a risk assessment. The risk assessment reveals that the chosen product vendor is actually a third-party integrator and does not directly provide any of the required services, but rather, use a third-party for each of the service offerings.

AIO does not have a formal risk management process in-house and lacks sufficient cyber expertise to identify risks associated with using the new platform. The third-party integrator for the AIO-identified product serves as a single source supplier, offering limited visibility and access that would allow AIO to better understand the supplier's cybersecurity

posture. This increases the risk of potential disruption to AIO operations should AIO experience a cyber incident as a result of a vulnerability in the third-party integrator's product. Although there are ICT related risks that have not been fully identified or mitigated, AIO executive management, against the advice of the CISO, decides to proceed with the integrator's proposed solution to speed up implementation of the new product for their customers.



ICT SUPPLY CHAIN RISK CATEGORIES

1//CYBER EXPERTISE
While the AIO CISO and IT team members have technical backgrounds in network engineering, administration, and software development, they lack specific cybersecurity expertise that would enable them to recognize third-party risks that could be harmful to AIO.

2//EXECUTIVE COMMITMENT
AIO's executive management's commitment to risk-based decision making has been superseded by the pressure to get a product in place quickly even though the potential ICT risks that the product may present are not fully known or understood.

3//ICT SUPPLY CHAIN RISK MANAGEMENT
While AIO has a CISO, none of the IT team members have general enterprise risk management or supply chain risk management backgrounds or experience.

4//SINGLE SOURCE SUPPLIER
The third-party integrator serving as a single source supplier presents a heightened risk to AIO as it becomes solely dependent on one integrator who has the ability to limit where and when AIO has access to the integrator's products and services.

5//SUPPLIER DISRUPTION
Every supplier inevitably experiences a service disruption. This will likely be true for the third-party integrators. Such a disruption would not only impact AIO, but also AIO's end customers.

6//SUPPLIER VISIBILITY
The reluctance of the third-party integrator to provide AIO with appropriate visibility and access to understand their potential ICT supply chain risks is a red flag and may point to their inability to demonstrate their cybersecurity posture.

POTENTIAL OPTIONS FOR AIO

Engage an outside consultant with risk management and cyber expertise in ICT supply chain risk management to conduct a risk assessment of the third-party integrator and identify, prioritize, and develop mitigation strategies for high priority risks.

Continue the search for a vendor that offers all of the requested services natively for an acceptable fee.

Perform the integration work in-house and hire staff that are qualified to conduct a risk assessment.

Establish a Service Level Agreement (SLA) with the integrator which captures uptime requirements and provides specific financial consequences when not meeting those requirements.

COST AND BENEFITS

POTENTIAL COSTS
Independent outside consultant hourly rates can range from $75/hour–$250/hour.

- The costs of recruiting and hiring in-house staff with cyber expertise and risk management experience will likely cost several thousand dollars plus compensation.
- Developing an SLA will take days to weeks to complete and may require the assistance of an independent consultant or legal counsel with expertise in drafting SLAs.

POTENTIAL BENEFITS

Engaging an independent consultant provides AIO access to ICT SCRM expertise on an as needed basis versus the costs of a full-time internal hire.

- Identifying a new vendor that addresses all of the ICT related requirements reduces the risk of exposure to AIO.
- Establishing an SLA with the integrator helps hold them accountable for their performance with monetary consequences should their product fail or cause damage or disruption to AIO.

RESOURCES

CISA: Cyber Security Evaluation Tool (CSET®)
CISA: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses
CISA: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services
DNI: Supply Chain Best Practices
NIST: NIST Small Business Cybersecurity Corner
NIST: Software Security in Supply Chains: Enhanced Vendor Risk Assessments

The National Risk Management Center (NRMC), Cybersecurity and Infrastructure Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are available at https://www.cisa.gov/national-risk-management.

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure
Security Agency
U.S. Department of Homeland Security

NRMC@hq.dhs.gov

For more information about NRMC, visit
www.cisa.gov/national-risk-management