REDUCING ICT SUPPLY CHAIN RISK IN SMALL AND MEDIUM-SIZED BUSINESSES

OVERVIEW

According to the Small Business Administration, there are over 31.7 million small and medium-sized businesses (SMBs) across the United States, which account for 41.7 percent of private sector employees and nearly half of the nation's gross domestic product. Given the importance of information and communications technology (ICT) products and services to SMBs and that many do not have dedicated risk management experts or functions internally, the Cybersecurity and Infrastructure Security Agency's (CISA's) ICT Supply Chain Risk Management (SCRM) Task Force developed the Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks. This resource details the most common ICT supply chain risk challenges faced by SMBs and provides practical and actionable measures they can take to mitigate these risks.

ICT SUPPLY CHAIN RISKS FACED BY AN SMB

A variety of approaches and techniques were used to gain insight into the highest ICT supply chain risk categories commonly faced by information technology (IT) and communications SMBs. Part of that process included a focus-group made up of communications SMBs, conversations with various industry groups, government agencies, and subject matter experts. The Task Force Working Group also received feedback from approximately 100 IT SMBs, 64 percent of whom had 100 or fewer employees. The following six categories emerged as the highest priority ICT supply chain risk categories for IT and communications SMBs:

- **Cyber Expertise**: The availability of knowledge, skills, and experience necessary to establish, implement, and manage ICT SCRM practices within SMBs. Collaboration is a key factor for an SMB to invest in cyber expertise most effectively.
- **Executive Commitment**: Company leadership, awareness, and knowledge of the business risk that cybersecurity breaches pose is critical, as well as 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.
- **ICT Supply Chain Risk Management**: Processes and practices ensuring the integrity of an organization's supply chain aimed at improving a company's cybersecurity practices by identifying, assessing, and mitigating the risks associated with information technology products and services are critical. This can include engaging relevant stakeholders, investing in the appropriate resources to protect the company's data, and integrating cybersecurity practices into a company's decision making, budget, and operational processes.
- **Single Source Supplier**: Suppliers who are preferred for a particular product or service or are a sole supplier of a given product or service.
- **Supplier Disruption:** 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.
- **Supplier Visibility**: The need for visibility into third-party cybersecurity practices.

MITIGATION AND ACTIONABLE MEASURES

In order to provide guidance that is practical, accessible, and usable by the SMB community, the resource handbook provides six use case examples, listed in Table 1, that illustrate common ICT supply chain risk challenges and actionable measures to mitigate these risks. The handbook was designed to provide ICT supply chain guidance to SMBs that may have limited finances and provides resources on how to vet ICT products and services that SMBs are considering for purchase. The handbook also offers methods and guidance on how best to tackle the most common and highest priority risks faced by SMBs.

Below are the use cases detailed in the handbook.

Table 1: Fictional Use Cases

Fictional Companies	Key ICT Supply Chain Risk Categories Addressed
Rural Utility Services (RUS): Broadband Service Provider	• ICT Supply Chain Risk Management • Supplier Visibility
Micro Coding Wizards (MCW): Software Company	• ICT Supply Chain Risk Management • Supplier Visibility
Cloud Information Systems (CIS): IT Company	• Executive Commitment • Supplier Disruption • ICT Supply Chain Risk Management
GreyCo: US Defense Integrator	• Executive Commitment • ICT Supply Chain Risk Management • Supplier Visibility
SubZeroQ: Quantum Computing	• Single Source Supplier
AIO Company: ICT Provider	• Cyber Expertise • Executive Commitment • ICT Supply Chain Risk Management • Single Source Supplier • Supplier Disruption • Supplier Visibility

Within each use case, several key risk factor elements are provided for reference, including:

- One or more of the six risk categories
- Potential options for the company to consider, to mitigate each specific risk
- A short summary of the costs and benefits of the actionable mitigation steps
- Accessible government and industry mitigation resources

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

RESOURCES

- ICT Supply Chain Risk Management Task Force: CISA.gov/ict-scrm task-force
- ICT Supply Chain Library: CISA.gov/ict-supply-chain-library
- ICT SCRM Task Force Resources: CISA.gov/ict-scrm-task-force-resources