FORTRESS

EBOOK

6 Steps to Managing Supply Chain Cyber Risk

1

Understand the environment.

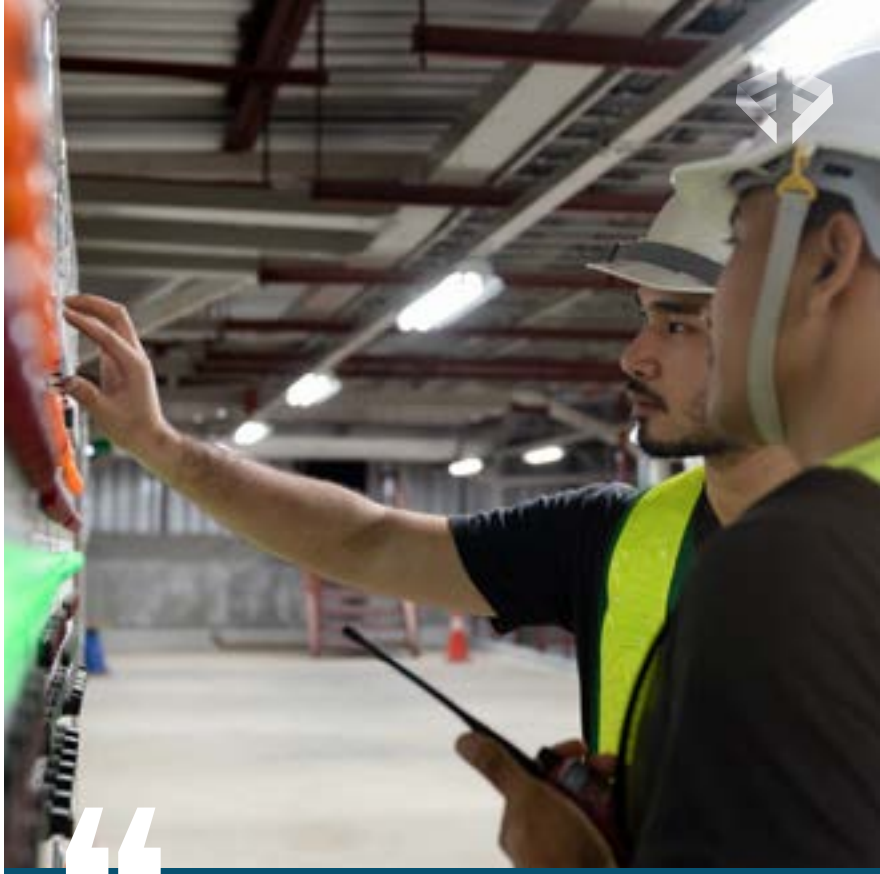
Today organizations rely more and more on partners and subcontractors for critical products and services.

This reliance provides benefits, but it also results in a disconcerting lack of visibility for those organizations as they lose full control of the product manufacturing of the services they provide. The resultant outcome is an increased vulnerability to network intrusions, hacks, and more sophisticated cyber-attacks. U.S. organizations incur the greatest cybersecurity risks and costs compared to their global counterparts. According to research, the cost of cyber data breach in the U.S. averaged $8.64M per incident compared to $3.86M for the rest of the world.

U.S. COST OF CYBER DATA BREACHES VS. THE WORLD

$8.64M

$3.86M



The threat is coming from 15 different vectors—Russia, China, North Korea, independent actors, the dark web and ransomware…among others. This is the hottest topic we've got as a country, and I think everybody's running scared right now on this issue. I think they're looking for solutions. Fortress is the solution—we deliver assets and capabilities that nobody else has today. Period.

Vice Admiral Albert Thomas "Tom" Church III
U.S. Navy (ret) Fortress Advisor, former Navy Inspector General

2

Learn from the experts.

To succeed and stay secure, companies and government entities should heed the National Institute of Standards and Technology (NIST) Cyber Supply Chain Security Principles.

Organizations must develop defenses based on the understanding that their systems will be breached.

When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.

Cybersecurity is never just a technology problem; it's a people, processes, and knowledge problem.

Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.

There should be no gap between physical and cybersecurity.

Sometimes adversaries exploit lapses in physical security to launch a cyber-attack. Additionally, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

3

Know the risks.

As the world has recently witnessed, network breaches have the potential to cause personal and financial loss, compromise to product integrity and safety, loss of life, and national panic.

These breaches threaten national security and personal well-being, to say nothing of the threat to myriad industries across the globe. Organizations can no longer protect themselves by simply securing their own infrastructures since their electronic perimeter is no longer meaningful, as threat actors intentionally target the suppliers of more cyber-mature organizations to take advantage of the weakest link.

When a supply chain is compromised, its security can no longer be trusted, whether it involves a chip, laptop, server, other technology, non-electronic product, or a service. This has become one of the most significant challenges facing government and business leaders today.

Recent intrusions into the Defense Industrial Base's supply chain have enabled foreign adversaries to gain backdoor intelligence into U.S. government affairs. This has spurred a new wave of regulatory action in the U.S. that will likely continue for the foreseeable future and is already beginning to expand to other global allies.

U.S. lawmakers and regulators continue to develop and implement new supply chain risk management regulations that will continue to impose very complex requirements for all government suppliers, contractors, and grantees.

Industrial control systems in many of our critical industries and companies are woefully antiquated. We have to use the infrastructure we have that's riddled with vulnerabilities, probably with malware, and root out stuff while we develop new techniques. We must rethink our strategies, tactics, and ways. Fortress works with the government and industry to drive the conversation forward.

Karl Wagner, Fortress advisor and former Chief of Counterintelligence Operations at the Central Intelligence

Know the risks.

The following are examples of how adversaries have accessed critical IT and OT systems:

- Third party service providers or vendors—from janitorial services to software engineering—with physical or virtual access to information systems, software code, or IP.
- Poor information security practices by lower-tier suppliers.
- Compromised software or hardware purchased from suppliers.
- Software security vulnerabilities in supply chain management or supplier systems.
- Counterfeit hardware or hardware with embedded malware.
- Third party data storage or data aggregators.

Tony Turner, VP of Security Solutions explains what an SBOM is and introduces a strategy for managing the copious amounts of data they provide

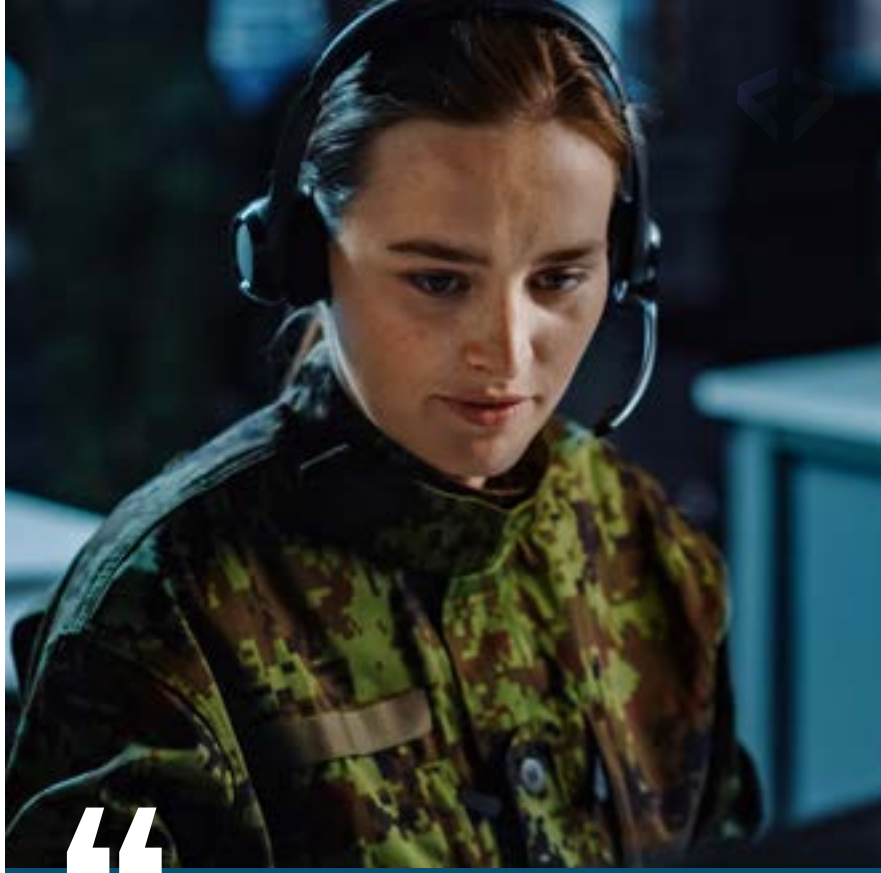
4

Ask the tough questions.

More rigorous regulations will help improve national security and hopefully reduce collective risk, but they do not alleviate individual companies from being diligent in determining their own supplier and subcontractor vulnerabilities.

Companies must be willing to ask candid, pointed questions of themselves and business partners:

- Is the vendor's software / hardware design process documented? Repeatable? Measurable?
- How does the vendor stay current on emerging vulnerabilities? What are vendor capabilities to address new "zero day" vulnerabilities?
- How is configuration management performed? Quality assurance? How is it tested for code quality or vulnerabilities?
- What steps are taken to "tamper proof" products? Are backdoors closed?
- How secure is the distribution process?
- What levels of malware protection and detection are performed?



"Having a common operational picture that everyone can see and ask hard questions from is the first step. Awareness matters. I would strongly recommend Fortress to base commanders or business leaders looking for that common view. They have the ability to come in and show you your vulnerabilities, where your soft spots are ... and then help you figure out how to best address those problem areas.

Major General Mark J O'Neil, U.S. Army (ret.)
Fortress Advisor and former commander of U.S. Army Alaska

Ask the tough questions.

- What physical security measures are in place? Documented? Audited?
- What type of employee background checks are conducted and how frequently?
- What security practice expectations are set for upstream suppliers? How is adherence to these standards assessed?
- What controls are in place to manage and monitor production processes?
- Have approved and authorized distribution channels been clearly documented?
- What is the component disposal risk and mitigation strategy?
- How does vendor assure security through product life-cycle?
- Is the mitigation of known vulnerabilities factored into product design (through product architecture, run-time protection techniques, code review)?
- What access controls, both cyber and physical are in place? How are they documented and audited?

4

5

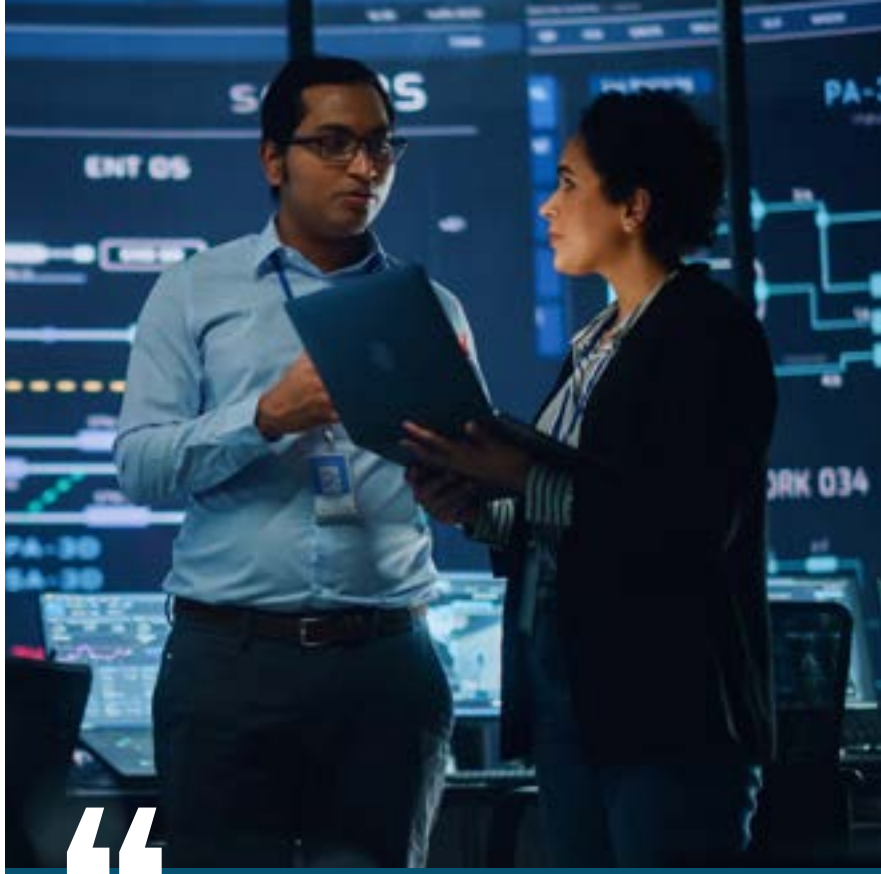
Partner for success.

Fortress Information Security brings extensive utility and federal experience in compliance, security, and risk mitigation to help clients identify and reduce vulnerabilities before they affect security, schedule, or profitability.

The Fortress team provides supply chain illumination solutions to deliver needed safeguards against expanding nation-state and criminal threats—while also ensuring compliance with current and growing regulations and best practices.

Identification of a problem is helpful, but it's only one part of the equation. Fortress' ability to find and implement cost and time-saving fixes is what sets us apart from competition that are long on promises and short on solutions.

Fortress cofounders Alex Santos and Peter Kassabov discuss a more holistic approach to supply chain security.



Understanding new requirements and regulations can be time consuming and costly without a partner that understands both the threat and regulatory environment. This is a daunting and complex process, and companies need answers that make sense. Furthermore, they need verification of initial findings and a "cradle-to-grave" continuity along the path to cyber hygiene and security.

Peter Kassabov, Executive Chairman and Co-founder at Fortress Information Security

Partner for success.

With Fortress' help, companies have adopted a variety of practices that help them manage their cyber supply chain risks. These practices include:

- Security requirements are included in every RFP and contract.
- Once a vendor is accepted in the formal supply chain, a security team works with them on-site to address any vulnerabilities and security gaps.
- Secure Software Lifecycle Development Programs and training for all engineers in the life cycle are established.
- Source code is obtained for all purchased software.
- Automation of manufacturing and testing regimes reduces the risk of human intervention.
- Track and trace programs to establish provenance of all parts, components, and systems.
- Programs capture "as built" component identity data for each assembly and automatically links the component identity data to sourcing information.
- Legacy support for end-of-life products and platforms assures continued supply of authorized IP and parts

6

Recognize the problem is not going away.

As the threat and corresponding counter-measures expand, even business units and suppliers that have nothing to do with the U.S. Government can put an organization at risk. Partnering with Fortress positions organizations to lead a risk and compliance data exchange that supports the intent of the new regulations and demonstrates a commitment to security, driving down cost and wasted time.

Fortress has a proven record of protecting critical infrastructure by managing these complex supply chain risks. As the threat continues to mature and evolve, and as the world's attention is drawn to the true gravity of cyber-attacks on the economy and quality of life, Fortress will continue to provide solutions in this environment.

THE NUMBERS

5K
average third party entities used by industry leaders

83%
of orgs have had a third party cyber insident in the last three years

51%
of orgs say they're not assessing third-party risk

A total risk mitigation solution

Fortress helps complex enterprises discover, prioritize, and monitor third-party security and cyber risks. We are the only company offering services and a customizable platform to manage OT, IT and third-party technology threats in a single end-to-end solution.

We provide risk management solutions for mission critical supply chains including services for vendor risk management, asset risk management, product security, file integrity, procurement, continuous monitoring, assessments, and remediation to support overall third party cybersecurity and integrity.

FORTRESS

CONNECT WITH FORTRESS