Why are ISO 28000 and ISO 20243 Important to Supply Chains?

RELIABLE PROCESSES IN SUPPLY CHAIN RISK MANAGEMENT

Data security breaches impact a company’s revenue and reputation alike, with customers leery to spend their money at a company that has been hacked, exposing private customer data. In 2016, there were 1,093 reported data breaches, which is a 40% increase from 2015.¹ Two of the biggest data breaches to make the news were from Target and Dun and Bradstreet, respectively.

Target’s data breach from 2013 made headlines when criminals gained access to 11 gigabytes worth of data—including customer credit card numbers, debit card numbers, and other private data.² This breach occurred due to a heating, ventilation, and air conditioning (HVAC) company that was doing work for Target and was given network access. Unfortunately, the HVAC company didn’t follow information security best practices, which led to an easy-to-breach database. Because of this, hackers could get their hands on and compromise that HVAC company’s credentials, including logins, passwords, and security badges. In the process, they gained entry to Target’s confidential private data.

For Dun and Bradstreet, in March of 2017, their marketing database with the contact information for over 33 million people was hacked and shared online.³ Dun and Bradstreet has strong security systems in place, so their own systems weren’t breached, but one of the thousands of partners who had purchased the list did not follow security best practices. Because of that lack of security, their system was attacked, which broadcasted the listings of the corporate contacts, including full names, work emails, phone numbers, and other confidential data.

With the right supply chain risk management (SCRM) policies and security standards like the ISO 28000 and ISO 20243 in place, as well as investing in security-rich computers, like the HP Elite family of products, powered by Intel® Core™ i7 vPro™ processors, there’s less chance of data loss and compromise via third parties.
ISO 28000 and ISO 20243 Explored

ISO 28000:2007 is an international standard that states the specific requirements for a security management system, including those parts that are critical to SCRM. Security management is a key component of many other aspects of a business, including business management, and these aspects include all activities that are controlled or influenced by organizations that impact supply chain security.

- Establish, implement, maintain, and improve a security management system
- Assure conformance with a stated security management policy
- Demonstrate that conformance to others
- Seek certification/registration of the company’s security management system by an accredited third-party certification body
- Make a self-determination and self-declaration of conformance with ISO 28000

Along with ISO 28000, SCRM is also involved in the ISO/IEC 20243:2015 Open Trusted Technology Provider Standard—Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) v 1.1. This is one of the first standards to assure the integrity of commercial off-the-shelf (COTS) information and communication technology (ICT) products, which leads to the security of your supply chain.

Counterfeit products, or ones that have been maliciously tampered with, pose a significant threat to companies through the potential introduction of untracked malicious behavior. This hacking can damage both customers and suppliers, resulting in failed or inferior products, revenue and brand equity loss, as well as disclosure of intellectual property. Governments and enterprises have begun to seek assurance that the products they use, like the HP Elite family of products, powered by Intel® Core™ i7 vPro™ processors, are secure, so providers of COTS ICT focus on protecting the integrity of products and services both in-house and as they move through global supply chains.

Becoming ISO 28000 and ISO 20243 certified is critical for a company’s security, and that holds especially true at CyberCore Technologies. CyberCore’s President & CEO Tina Kuhn, states “We have increased the security of the supply chain for our customers and our ISO 28000 certification mitigates the persistent risk of counterfeit or tainted product. It is imperative that organizations, large and small, commit to understanding and managing the supply chain cybersecurity risks that have become top of mind for executive leaders, boards, and consumers across the globe.”

“We have increased the security of the supply chain for our customers and our ISO 28000 certification mitigates the persistent risk of counterfeit or tainted product. It is imperative that organizations, large and small, commit to understanding and managing the supply chain cybersecurity risks that have become top of mind for executive leaders, boards, and consumers across the globe.”

- Tina Kuhn, President & CEO of CyberCore Technologies
Prevent Data Breaches

With all the confidential data stored in a company’s databases, it’s critical to prevent attacks on smaller partners in supplier and partner networks. These partners are easy targets for hackers when the business they’re looking to infiltrate already has a solid in-house security program implemented. How can you work to protect your data from these attacks?

- Look at the information security practices throughout your entire network up and down your supply chain
- Make a choice to only work with suppliers and partners that have security as one of their top priorities
- Work with your suppliers and partners to collaborate on security and create a coordinated security plan
- Update your security practices to defend against the types of third-party attacks that hit Target and Dun & Bradstreet
- Shore up your security measures to make it harder for hackers to further compromise already breached systems or individuals

CyberCore’s corePROTECT insider threat solution is specifically engineered to safeguard your organization in today’s digitally connected environment. This solution helps secure your endpoints and confidential data by alerting administrators when suspected malicious activity is detected from third-party supply chain partners or other potential intruders.

We take powerful third-party monitoring software and tools and combine them with our extensive security expertise and in-depth knowledge of your business processes to provide comprehensive and robust end-point security monitoring. corePROTECT defends your network and the HP Elite line of desktops, laptops, and tablets, strengthened by Intel® Core™ i7 vPro™ processors, against external attacks, malware, viruses, and unpatched firmware and software exploitations with these features:

- Real time, continuous monitoring 24x7x365 out of CyberCore’s Cyber Security Operations Center (CSOC)
- Vulnerability assessments and penetration testing
- Intelligent analysis and alerts of suspicious activities
- Customizable monitoring and analysis rules to support your organization’s policy
- In-depth capture of forensic evidence for litigation cases

SCRM is so important to a company, as supply chain failures that impact your PC purchase can also be detrimental to your company’s operations, plans, and revenue through a data breach like the ones that affected Target and Dun & Bradstreet. Not to mention the harm that can come to intellectual property and primary technical systems.

CyberCore protects your purchase of PCs like the HP Elite family of products, powered by Intel® Core™ i7 vPro™ processors, from these supply chain risks:

- Data breaches
- Product tampering
- Counterfeit components
- Hardware/software sabotage
- Theft and piracy

With a Security Risk Assessment Process in place, you know what information is being accessed and ensure the data is being handled safely. corePROTECT not only complies with all Department of Defense (DoD) regulations, but as your third-party vendor, our ISO 28000 certification provides verified regulatory compliance value to your organization.
Protect Endpoints for Supply Chain

Your supply chain is most vulnerable at its endpoints. That’s why HP Elite notebooks, desktops and tablets, powered by Intel® Core™ i7 vPro™ processors, incorporate a comprehensive set of security solutions focused on protecting not only the device, but also the user’s identity and data:

- HP Sure Start Gen3 protects the BIOS from malware attacks both in pre-boot and run-time
- HP Sure View integrated privacy screen thwarts visual hacking
- Advanced biometric security features like fingerprint and iris recognition

Don’t take a chance on gray market components or infected PC software that have the potential to harm your operational integrity, steal your intellectual property, and sabotage your business. HP Elite notebooks, tablets, desktops, and monitors offer best-in-class security and are built to exacting standards with industry-leading features that keep your business moving seamlessly and efficiently.

When you use corePROTECT’s insider threat client on HP Elite desktops, laptops, and tablets, strengthened by Intel®, you add an even greater layer of protection. Features like device connection analysis, file location, data-at-rest reports, file transfer protection, secure print services, and content monitoring give your organization the maximum level of security and insight.

Contact us at 410-560-7177, or visit www.CyberCoreTech.com to learn how our customizable suite of Insider Threat Monitoring Solutions can secure your investment in HP Elite Series products.


The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel Inside®, Powerful Productivity Outside.

Intel, the Intel logo, Intel Core, Intel vPro, Core Inside and vPro Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

Copyright © 2017 CyberCore Technologies