DIGITAL DEFENCE

Virtual CISO Program –

Securing the Supply Chain

Advise
Service

OVERVIEW

As businesses become more interconnected in the global marketplace, they are forging relationships with extensive networks of third party vendors in vast and complex supply chains. Unfortunately, these chains are only as secure as the weakest link.

Cyber attackers are focusing on these vendors because while traditional network are resilient against attacks, many suppliers are smaller, and they lack the resources to ensure the privacy and security of data that has been trusted to them. To secure their supply chain, businesses have to overcome multiple challenges, including:

- Business lack visibility into the sensitive information that is shared with the supply chain, both directly and by automated processes
- There is a lack of knowledge regarding required security controls, and an accompanying end-to-end understanding if the controls have been put in place
- As businesses become more interconnected within the global marketplace, their supply chain is impacted by different laws and business cultures
- Frequent changes in suppliers and products
- Multiple contracts and other agreements provide inconsistent protection

To resolve these issues, DigitalDefence has developed the vendor security management service to secure the flow of data across an organization and its partners.

BENEFITS OF A VENDOR SECURITY ASSESSMENT:

The benefits of a vendor security assessment include:

- "Quick Start" approach ensures rapid and cost-effective protection against attacks originating from trusted partners who may have been compromised

Improve corporate risk reduction with strategic security and privacy services.

Is the Vendor Security Management Service right for your company?

- If your supplier was compromised by a hacker, would you be protected from an attack originating from such a "trusted" site?
- Up to 80% of data breaches, including those of Target and Home Depot, originate in the supply chain. Are you and your partners prepared for an effective, coordinated incident response?
- Are you aware that securing your supply chain could reduce cyber-insurance rates and corporate liability?
- Can you meet regulatory requirements for supply chain security as defined by ISO 27001, PCI DSS, and other standards?
- Do you know if your suppliers protect your company's data as diligently as you protect it?

- Customized and comprehensive program protects your sensitive corporate data no matter where it resides
- Ensure compliance with regulatory requirements, reduces overall liability, and may decrease costs of cyberinsurance

We ensure that your supplier chain protects your data with the same diligence that your own organization relies on.

SERVICE DESCRIPTION

DigitalDefence works with each client to tailor a specific vendor supply management program. Typically, the program will include:

- The starting point of each program is to conduct a Vendor Risk Assessment for your organization. We will:
  - Identify who your vendors are, and which ones are critical to your success
  - Define the security and privacy requirements for your data
  - Review the policies and procedures governing your relationships with third parties, especially around incident detection and response
  - Review contracts and other protections against loss due to third party actions
  - Communicate these requirements to all members of your supply chain
- We will work with smaller suppliers to complete a Facilitated Scorecard—an easy-to-understand document shared between you and the vendor that defines how security and privacy are being controlled. Because we validate the risks and controls reported on the Scorecard with the vendor, you can be assured that the information is an true representation of your current state. All security gaps will be highlighted, ensuring that they can be promptly and effectively addressed.
- For larger vendors, or ones judged to be most critical to your business success, we will go on-site and complete a Vendor Site Assessment of the risks and security controls in place. This assessment will go beyond simple questionnaires—it will provide an accurate picture of the current state, and on-going metrics to confirm compliance with your security and privacy requirements.
- The final step is to establish and maintain a Vendor Management Program within your organization. Using our online security awareness portal, this program will provide a shared knowledge environment between your organization and the vendor supply chain to ensure that all members are effectively securing data. It will also provide for shared performance metrics that can be used to validate the continued success of the program and to support regulatory and cyberinsurance requirements.

According to a 2015 Verizon study, 40% of attacks spread from the initial target to hit a second organization in less than 1 hour; 75% of attacks hit a connected partner organization within a day

Are you protected from your suppliers?

About DigitalDefence

DigitalDefence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

DigitalDefence Inc.
Toll-Free 800-385-1632 | Tel 519-771-8808
info@digitaldefence.ca | www.digitaldefence.ca