Security Awareness in Business: Who Me?

Tuesday, February 23, 2016

Any successful business–small or large–exists based on revenue growth and loss prevention. We all have seen cases where criminals, spies, and terrorists have targeted businesses. Vulnerabilities in physical, supply chain or cyber security can cause down-time and loss of business and reputation if such situations are not handled appropriately and quickly. This may, in turn, impact the company's bottom line and ultimately impact profits. Further, prohibited or restricted imports or exports can lead to confiscation of goods, penalties, and poor public perception by clients as well as government agencies.

Security Comes First

Firms often find the task of keeping the business functions aligned with security processes highly challenging, especially during economic downturns. However, the reality is that security should be a primary issue. For example, a computer virus outbreak or a network breach can cost your business thousands of dollars. In some cases, it may even lead to legal liability and lawsuits.

Awareness and Knowledge

Identifying, managing, and exploiting risk across an organization and throughout the global supply chain—from product development to receipt and payment—has become increasingly important to the overall success and longevity of any business. The first defenses are awareness and knowledge.

A part of operations security is a precautionary step known as a general risk assessment. This assessment would include protecting proprietary information that would cause harm. In addition, these assessments defend against threats from criminals, terrorists, and others from obtaining goods or discovering critical information about company's activities, business processes, or employees.

Important Steps in Security

1. Complete a Risk Assessment

- identify parties responsible for conducting the assessment
- analyze all possible threats
- quantify and document risks
- apply countermeasures
- monitor your results

2. Develop Company Policies

A. Operations Security

- secure on-site and offsite property/goods
- document inventory controls
- monitor third party providers (i.e truckers, warehouses and employees)

B. Physical Security

- plan and map escape routes
- address procedures for backup generators and off-site backup I.T. systems
- secure documents in locked cabinets and document shredding
- secure single monitored public entrance, cameras, access controls and monitoring by outside services
- process visitors, maintain logs and escort guests

Note: FEMA recommendations are published in technical reports/bulletins and training on building science including building codes, flood proofing, earthquake standards, wind design requirements, etc.

C. Training on security incidents, natural disasters, and cyber security

- provide awareness training for employees, including those travelling abroad
- conduct monthly audits
- develop a crisis communications policy for key personnel
- periodically review and update disaster recovery plan

D. Insurance

- insure flood and fire damage
- insure inventory equipment
- insure employees' laptops, mobile devices, USB's etc.

E. Human Resources

- establish an employee screening policy
- maintain a list of emergency contacts (management, local emergency services), employee escape routes, first aid equipment, fire extinguishers, emergency tool kits, flashlight, batteries and

firearms (if permitted)

F. I.T.

- keep a log of hardware/equipment
- develop security protocols for network access
- document procedures for monitoring/detecting malware, viruses, etc.

G. Supply Chain Security

- follow best practices for container seals
- develop standard operating procedures for supply chain partners and vendors
- map your supply chain from end to end

To learn more about security awareness in buisness and training on protecting your corporate identity, click here.

By Diane Cima

https://mohawkglobalta.com/security-awareness-business-me/