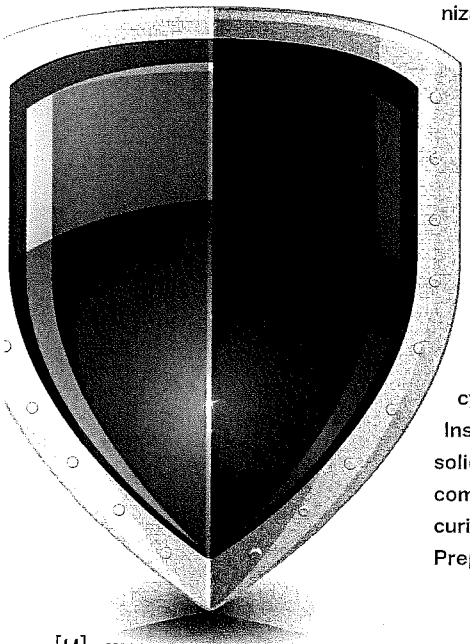
By Michelle Cohen

Best Offense Is a Good Defense

Supply managers must keep on top of ever-changing cybersecurity laws to protect their organizations and their customers.

Cybersecurity breaches at major companies grab headlines as legislatures and regulators at the state, federal and international levels develop "rules of the road" for protecting information, especially consumers' personal data. Supply management professionals should be concerned that their systems and/or employees may be exposing their organizations to data breaches — opening the company to lawsuits, governmental enforcement actions and significant reputation damage.



Suppliers throughout an organization's supply chain possess various forms of sensitive data, such as customer information, and corporate proprietary information, such as trade secrets.

Privacy and IT security experts advise companies and their supply management organizations that they should never consider themselves "shielded" from cyberattacks and data loss. Instead, the best offense is a solid defense — assume your company *will* suffer a cybersecurity breach of some type. Preparation is critical, followed by quick but careful actions that address certain important legal and business considerations. Every organization should consult its own IT group, legal advisers and public relations team for specific guidance.

Cybersecurity Consequences

We've all heard about hacking, where a third party breaches the network security (or lack thereof) of an organization. While hackers make the news, a significant portion of cybersecurity breaches originate within a company, and vary from employee negligence to a network security lapse that exposes data or disrupts the network (see *Defending Cyberspace, Inside Supply Management®*, December 2011/January 2012).

Whatever the type of cybersecurity event, the impact on a company's bottom line is hard to ignore. According to the Michigan-based Ponemon Institute, the average cost of a data breach for a victimized organization is about US$7.2 million.

Establishing Policies, Procedures

As a first step, businesses should ensure they have written policies and procedures to keep their networks and data secure. There is no one-size-fits-all policy. Each organization must evaluate the security of its networks (including mobile networks and cloud computing), the types of information the business collects and maintains, how it uses this information, who can access the information, how long the information is maintained and how it is destroyed.

Supply management organizations also need to understand and gain assurances from suppliers as to how they secure the data the organization is sharing with them. While written policies and procedures make good business sense, depending on your industry and the type of information your organization maintains, these procedures could be mandatory.

For example, does your business "own or license" — in other words, receive, store, maintain, process or otherwise have access to personal information in connection with the provision of goods or services or in connection with employment — of a Massachusetts resident? Even if it maintains only one Massachusetts resident's personal information, your company

is subject to Massachusetts' groundbreaking regulations mandating that, among other obligations, a written information security plan be in place. Key requirements under Massachusetts law include:

- Encryption of documents sent over the Internet or saved on laptops or flash drives
- Encryption of wirelessly transmitted data
- Deployment of up-to-date firewalls to protect company data.

Other provisions under the Massachusetts law, arguably one of the most stringent in the nation, are also good to keep in mind in connection with any written information security program, including:

- Immediately blocking terminated employees' physical and electronic access to personal information records, including deactivating their passwords and user names
- A reasonably secure method of assigning/selecting passwords, or the use of unique identifier technologies such as biometrics or token devices
- Requiring that hardcopy data containing covered information be stored in locked facilities, storage areas or containers, and accessible on a need-to-know basis
- Procedures for documenting any actions taken in connection with any breach of security
- A requirement for post-incident review of events and actions taken to improve security.

The Massachusetts checklist can be found at www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf.

Whatever the type of cybersecurity event, the impact on a company's bottom line is hard to ignore.

The federal Gramm-Leach-Bliley Act requires financial institutions to implement written security procedures to protect customer information. Companies covered by the Health Insurance Portability and Accountability Act also have information security procedure requirements as they relate to protected healthcare information. These are just a few examples of legal requirements for written policies and procedures governing cybersecurity; the list is by no means exhaustive.

Data Breaches/Losses

Despite an organization's best efforts, data breaches can and will occur. Most states require prompt notification to affected persons if their personal information has been exposed. The definition of personal information and the types of exposure vary. If faced with a breach or loss, a company (principally IT security, legal, communications, human resources and any other department directly affected) should take the following precautions.

Gather the relevant facts. Immediately determine what was breached or lost. Was it company financial information or employee/customer information? When did it occur? When did the company find out?

Determine action. Decide whether immediate steps need to be taken, such as changing passwords and notifying law enforcement, which is typical in outside hacking incidents.

Involve crisis management team. The data breach will go public, possibly viral. Be sure to check websites that monitor and publish information on data breaches, such as the Open Security Foundation (http://opensecurityfoundation.org).

Coordinate responses. Designate a central person/office to address inquiries and ensure consistency in your company's reaction and plan.

Prepare for notification. Determine what types of notifications may be necessary. Some states require notice to their attorneys general, other state agencies and the major consumer reporting agencies, in addition to affected individuals.

Prepare restitution. Determine what may be offered to affected persons. For example, free credit monitoring services are fairly standard.

Keep good documentation. Document all actions taken and any threats of litigation/enforcement actions.

Conduct an analysis. Analyze all remedial and corrective actions, including any network fixes or employee retraining.

Supply Chain Challenges

What if information your supply management organization keeps about one of its strategic suppliers is compromised? Legal requirements vary depending on the type of information stolen or compromised in a security breach. One rule of thumb is if the cybersecurity breach affects personal information, most states require your company to report the event promptly to the company whose information was compromised and to cooperate with the company in making required notifications to persons and regulators.

When information such as supplier contract or price negotiation information is compromised, the supply management organization should review all applicable contracts with the supplier to determine if contractual obligations require reporting to the supplier whose information was compromised.

Evolving Requirements

The legal requirements addressing cybersecurity continue to evolve. The Obama administration delivered a cybersecurity proposal to Congress in May 2011 that would require companies to report data breaches based on a national standard, toughen penalties for computer crimes and direct the U.S. Department of Homeland Security (DHS) to work with banks, utilities and transportation operators to develop cybersecurity plans. In November 2011, the Federal Communications Commission (FCC) launched the "Small Biz Cyber Planner," an online resource to help small businesses create customized cybersecurity plans. And Congress has introduced various cybersecurity bills, so it is wise to keep an eye on this changing legal landscape. **ISM**

Michelle Cohen is a partner and certified information privacy professional with Thompson Hine LLP in Washington, D.C. For more information, send an email to **author@ism.ws**.