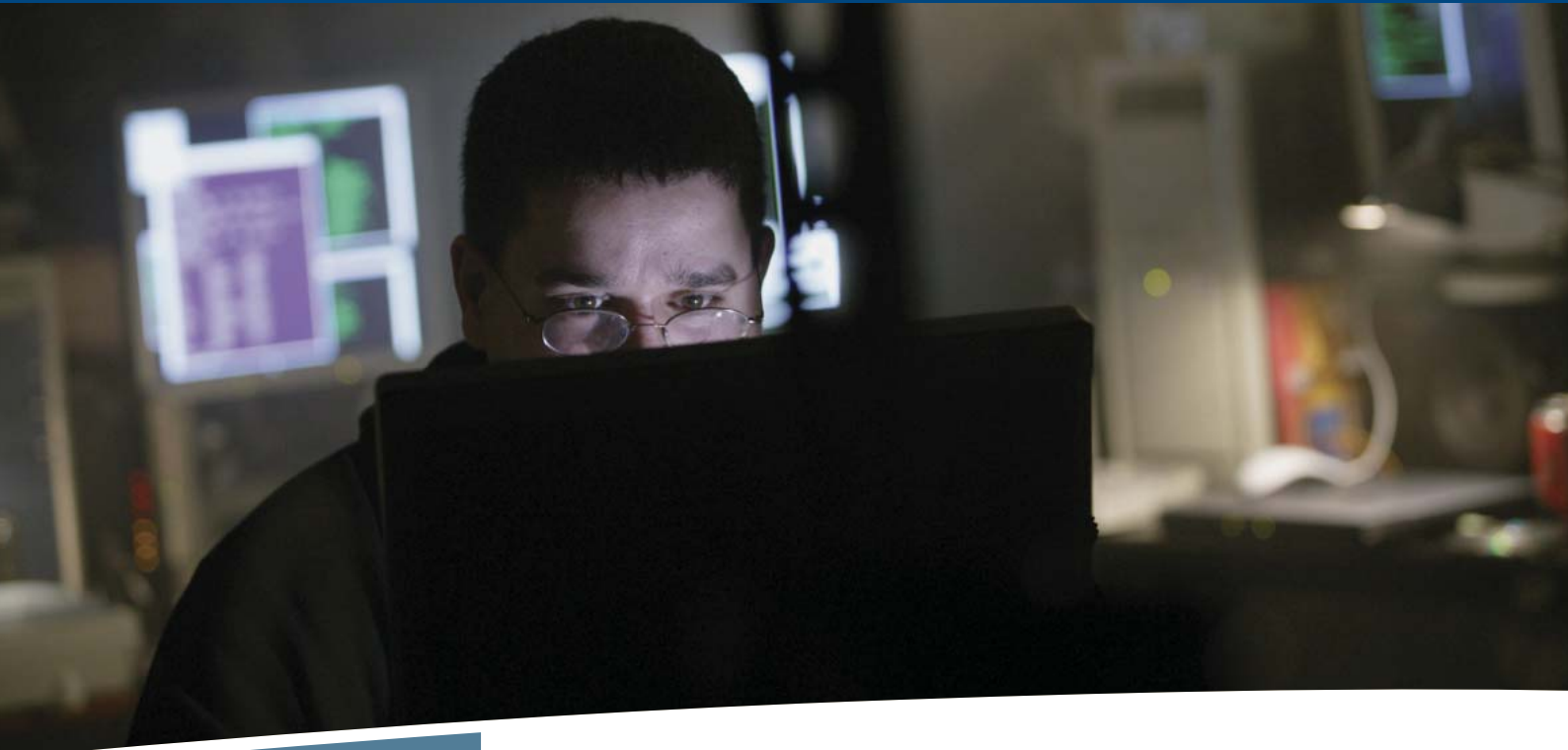


What should you do to prevent cyber thieves?



By: Lockton Technology, Media and Telecom Practice | Lockton Companies, LLC
Winter 2010



Hackers mount new strike

Many of our clients have seen and commented on the *Wall Street Journal* article of Feb. 18, 2010, entitled “Hackers Mount New Strike,” and the *USA Today* article on the following day, entitled “Stolen Logons In Hands of ‘Amateurs.’”

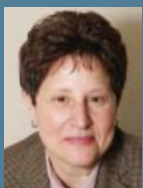
The *Wall Street Journal* article detailed the findings of a computer security company that hackers in Europe and China had successfully broken into computers at more than 2,400 companies and government agencies during the past 18 months in a coordinated global attack. The hacking operation is considered on-going and not fully contained.

This attack exposed vast amounts of personal and corporate sensitive information from credit card transactions to corporate trade secrets, contracts, presentations and source code of new products. A wide variety of companies have been potentially breached.

Hacking attacks involved criminal organizations not only located in the host country of the victim, but coordinated through multiple countries.

The methods of entry into corporate systems included:

- ❖ Social engineering ruses designed to trick employees to click on contaminated Web sites, e-mail attachments or seemingly innocent ads.
- ❖ Use of botnets—A collection of compromised computers that are controlled by the same hacker that is slowly built up and then unleashed as a denial of service attack, used to send spam or commit some form of computer crime. One security researcher reported that there are 2,000 botnet gangs that together control 5 to 7 percent of PCs in corporate settings in North America.
- ❖ Spyware infections such as ZeuS, or other forms of malicious code (malware).



Emily Freeman,
ARM, AIU
Executive Director, TMT
Lockton International—
London

Tel: 011-44-207-933-2224
E-mail: emily.freeman@uk.lockton.com



Ben Beeson
Executive Director, TMT
Lockton International—
London

Tel: 011-44-207-933-2857
E-mail: ben.beeson@uk.lockton.com

The article focused on the reality of the external hacker engaged in cyber war and/or cyber crime. There is also the reality of internal problems as well—the impact of recessionary times manifested in malicious or criminal acts by insiders, as well as user errors, lack of security awareness and lack of mobile device security.

Outsourcing and off-shoring of IT and other business functions continues as a global trend. However, there has been a significant rise of security breaches committed by vendors who host, process, store or handle customer and employee personal financial or healthcare data.

Many corporate executives mistakenly believe that by outsourcing the work to vendors, they have also transferred the liability that may arise from a data breach or system failure. Unfortunately, that is not the case. The legal and regulatory liability regarding security and privacy of personally identifiable non-public information, either medical or financial, primarily remains with the data owner, i.e., the client of the vendor.

“Many corporate executives mistakenly believe that by outsourcing the work to vendors, they have also transferred the liability that may arise from a data breach or system failure.”

How can you prevent your company from being compromised? What best practices should my firm consider?

Privacy and security risks definitely should be managed as a high severity risk management issue—involving claims, investigations and costs, but also loss of reputation and customer trust.

In the U.S., privacy violations and security breaches can result in civil lawsuits, frequently class actions. Some

international jurisdictions maintain stringent laws and regulations especially related to privacy, e.g., E.U. Data Privacy Directives.

At the front end of data breaches, there is an array of direct costs associated with computer forensics and mandatory notification to the affected individuals (customers and/or employees). Nearly every state has passed laws that call for organizations holding *non-public personally identifiable information* (PII) to notify the affected persons if their information has been potentially compromised, whether it occurred directly or indirectly through vendors. For healthcare providers and their business associates, there is also the federally required notification regarding *personally identifiable healthcare information* (PHI).

Our suggestions:

1. **Multifunctional approach**

This is not just an IT security issue, rather an enterprise risk management issue that involves not only IT, but also the risk manager/insurance manager, legal department, compliance, internal audit, procurement and operations. Get together as a team with the support of senior management to:

- ❖ Define activities and services that involve PII and/or PHI that put your organization at risk. What systems store PII and/or PHI? What would be the aggregate potential if such data were breached? Consider not only electronic data, but also paper records that contain PII/PHI.
- ❖ What outside vendors or business associates have access to PII and/or PHI? In selecting or renewing a contract with such vendors, what due diligence has been done to determine the state of their security and privacy controls? What has been done on vendor contractual controls and insurance requirements?
- ❖ Determine current state of risk prevention and mitigation and develop effective projects to improve these each year.

2. Comply with applicable standards, laws and regulations (ditto with vendors)

Security laws and regulations are not static—new legal and regulatory developments occur at a state and federal level, as well as around the world where you have operations or employees. In the U.S., there are major regulations regarding medical privacy/security (HIPAA/HITECH) and financial information privacy/security (Gramm-Leach-Bliley). You can stay in touch in a number of ways. One excellent way is the Web site of the International Association of Privacy Professionals, or you can join as a member—
www.privacyassociation.org.

If you are involved with credit card transactions, then it is critical to get in compliance with credit card association security requirements (called PCI DSS). Determine your merchant or processor level if applicable (refer to www.pcisecuritystandards.org)

3. Manage your high-risk vendors

Identify all your high risk vendors for security and privacy risks which includes credit card processors. Make sure these high-risk vendors are in compliance with industry standards or PCI if applicable (require such contractually) and include in your vendor contract strong indemnity/insurance requirements for data risks! Lockton can help with due diligence, contract clauses and insurance requirements.

4. Focus on people and processes, not just technology aspects of security controls

Physical security and technology tools (anti-virus, IDS, etc.) are an excellent part of a comprehensive approach, but focus as well on people and processes failures and potential for malicious acts. Staff security training and awareness, background checks, filters and controls of employee usage of the Internet, and strict role-based access to sensitive systems and confidential data should be on your list. Companies should take a hard look to ensure that there are no unauthorized Internet peer-to-peer (P2P) file-sharing programs on their network and that authorized programs are properly configured and secure internally. Avoid emailing PHI/PHI in the clear or via unsecure P2P programs.

5. Test your controls and fix vulnerabilities continuously

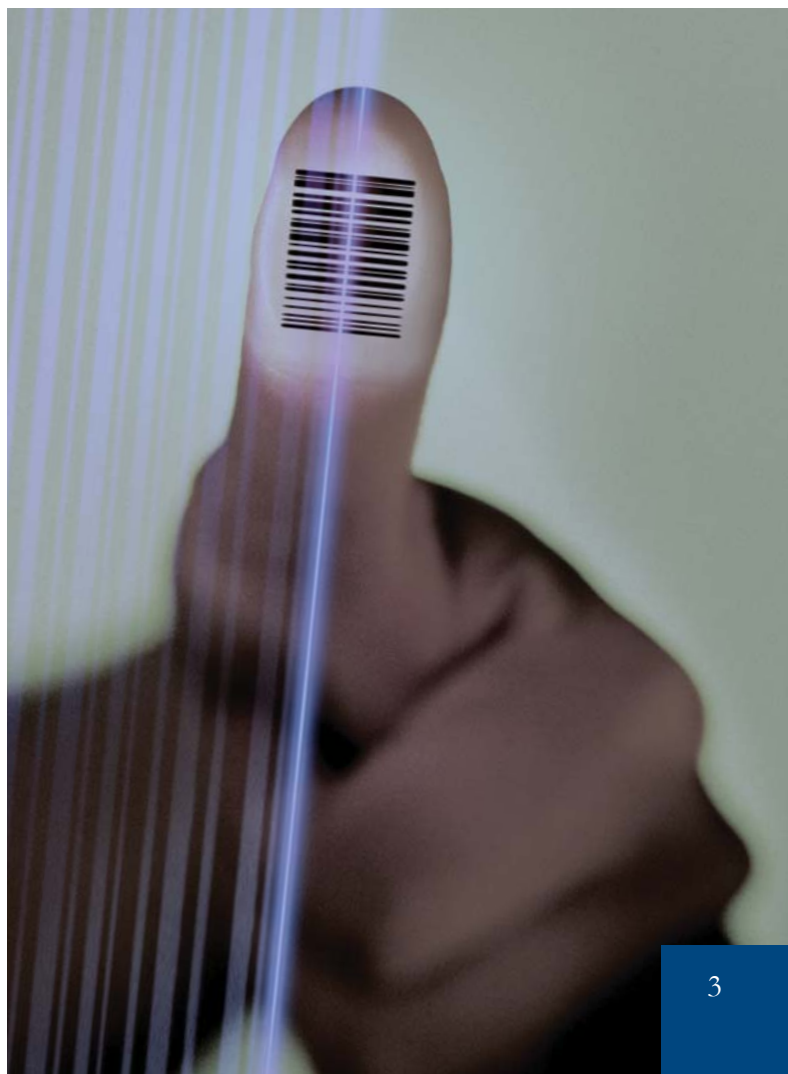
You cannot prevent criminals from trying to break in—you need to contain/minimize incidents and prevent actual breaches. Part of your plan should encompass not only internal testing and controls, but also include

periodic external scanning, penetration testing and process/control audits. Hire external security partners with experience in your industry. Lockton can recommend some excellent firms. Develop a patch management strategy and fix high-risk vulnerabilities promptly and patch all your servers.

“This is not just an IT security issue, rather an enterprise risk management issue.”

6. Encrypt sensitive data

Encryption is a key control—not only of PII or PHI at rest on your systems, but also in-transit or on mobile devices (laptops, tapes, USB pens, etc.). There are other methods, such as elimination, tokenization or masking, but having such data “in the clear” not only substantially increases the risk, but also may be prohibited by law or standards (PCI for example). Mobile devices are a major problem—preventing PII/PHI from being downloaded on such devices; or if absolutely necessary to have on a mobile device, then protect it through encryption.



7. Develop a security breach incident response plan

Your company has a contingency or mitigation plan for natural disasters and the like. This risk deserves to have a contingency plan particularly if your company accesses, processes, manages, stores or handles PII and/or PHI of third parties. Lockton can help you put one together along with our cyber insurance programs.

Managing risk through insurance

Lockton can review your own insurance program for cyber risks. Clients must protect themselves, as the ultimate responsibility lies with the data owner and there is the very real possibility that the vendor could commit a breach in security that could overwhelm them and their available insurance limits.

“Clients must protect themselves as the ultimate responsibility lies with the data owner.”

Our expertise and services at Lockton

At Lockton, we have a specialty in design, placement and management of technology, media, telecom and cyber risk insurance. We design insurance programs for both first-party risks (direct business interruption and extra expense associated with a breach/outage) and third-party liability on an integrated basis with other risks where possible (for example, combined with technology/miscellaneous professional liability) or on a stand-alone basis.

We have innovated unique line slips as well as specific wordings with underwriters amending their standard forms.

We uniquely have an insurance program to address reputational harm from a third-party data breach.

We also participate as needed with clients to explain the underlying risks, relevant claims and regulatory environment. Given our experience, we can provide valuable benchmarking information to assist in the discussion about limits and retentions. As there are no standard industry wordings, we highlight the differences in various policy forms and we have authored a number of manuscript changes to broaden the industry versions to better suit our clients' needs.

We assist our clients in preparing the necessary underwriting information to upgrade insurance or purchase insurance in areas where the client policies are not adequate.

Lockton corporate overview

Lockton is the world's largest, privately owned insurance broker. With more than 3,800 people, Lockton delivers seamless service to companies of all sizes, as well as to individual clients. The company was founded Kansas City, Missouri, USA in 1966, and has grown to become the tenth largest insurance brokerage firm in the world.

Lockton service teams can be found on four continents and in major cities in the United States, United Kingdom, Ireland, Latin America, Middle East and Asia. Through our European broker partnership with EOS RISQ and other alliances, Lockton serves clients virtually everywhere in the world.

For more information on what is available and what specific cyber insurance products best fit your needs, please contact your Lockton account executive or our Lockton Technology, Media and Telecom (TMT) Specialists.

