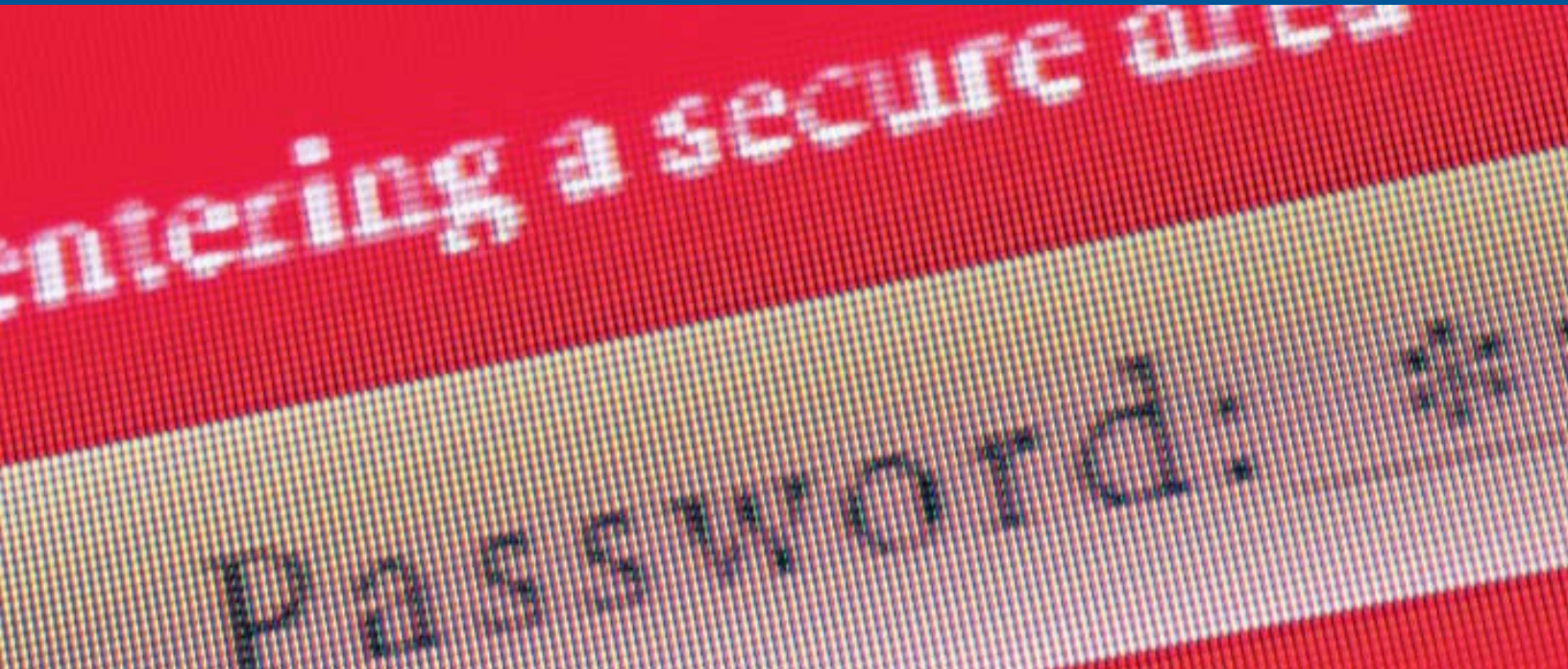


Cyber Liability— International

Market Update Spring 2010



Contact



Emily Freeman

Executive Director
Technology, Media, Telecom
London, U.K.

Telephone: +44 0(20) 7933 2224
E-mail: emily.freeman@uk.lockton.com



Ben Beeson

Executive Director
Technology, Media, Telecom
London, U.K.

Telephone: +44 0(20) 7933 2857
E-mail: ben.beeson@uk.lockton.com

Fighting Back Against Cyber Thieves

Chinese and European hackers have recently infiltrated more than 2,400 U.S. companies and government agencies. A group of amateur hackers discovered 68,000 stolen user names and passwords online. Between 12 percent and 15 percent of the 1.6 billion personal computers (PCs) connected to the Internet are controlled by cyber criminals. Two thousand “botnet” gangs collectively control 5 percent to 7 percent of the PCs within U.S. companies.

So, just how safe is your own corporate data and your customers’ data?

Whether it is a deliberate attack by cyber criminals or an employee randomly clicking on an infected download link, spyware—like the infamous ZeuS—or other malicious code poses an ongoing data security exposure. Tough economic times also increase the threat from disaffected employees. Outsourcing and off-shoring create risks too. Many executives believe liability for data breaches transfers to outsource providers. Wrong: liability stays with you, the data owner.

Losing track of customer data can be expensive. Beyond the financial impact of class actions or other civil lawsuits, there is the risk of major damage to your corporate reputation. Computer forensics and mandatory notification of those affected can cost £10 to £15 (\$15 to \$20)—per customer.

So what can you do to protect your company? First, recognize data security as a high-severity enterprise risk management issue. Then create a team comprising risk management, legal, compliance, internal audit, procurement, and operations to map your exposures.

Where is sensitive data held? Who has access? Have your partners and suppliers been fully vetted? What do their contracts look like? Do they hold appropriate insurance?

Be sure you comply fully with changing state, federal, and international regulations. This includes the HIPAA/HITECH (medical) and Gramm-Leach-Bliley (financial) data privacy regulations. If you process card payments you must also comply with PCI DSS.

Technology plays a major role, but consider also the human element. Focus on security training and awareness, background checks, filters, and controls on employees' online activity as well as strict role-based access to sensitive systems and data.

Check regularly for unauthorized peer-to-peer file sharing and be sure authorized programs are properly configured and internally secure. Never e-mail PHI/PII except through secure channels. Keep sensitive data encrypted on your systems—and on any mobile device—at all times.

Keeping cyber criminals out altogether may prove impossible. But combining internal testing and controls with periodic external scanning, penetration testing, and process/control audits should enable you to contain their incursions and prevent an actual data breach.

Should all this fail, you should have a security breach incident response plan in place to help you minimize the impact. Understanding what needs to be done in advance can make all the difference in the aftermath of a data security lapse. Seek expert advice to help you understand your risks and protect your business.

Lockton can help review your current exposures and assess how your existing insurance cover would respond—or not—should such risks materialise. At Lockton we specialise in the design, placement, and management of technology, media, telecom, and cyber risk insurance. We work closely with client companies to help them understand and contain their exposure to online fraud, data breaches, and other forms of cyber risk.

We create tailored programmes to protect against the direct costs of business interruption and additional expense associated with a data breach or system outage—as well as integrated programmes covering cyber risks along with other technology and professional liability risks. Working with leading insurance underwriters in this specialised field, Lockton has been responsible for creating unique new wordings to encompass emerging areas of cyber risk.

For additional information and the latest insights click on the links below.

What should you do to prevent cyber thieves? By Emily Freeman

Identity theft: urban legend or real risk? By Dan Hopkinson