<< Left
Jeffrey Blatt
Of Counsel
jeffrey.b@tilleke.com

<< Right
David Duncan
Consultant
david.d@tilleke.com

Cyber Security Preparedness: It's a Dangerous World Out There

Virtually all of us are dependent on the use of the Internet and Internet-connected devices. People are plugged in, online, and in constant communication through wired and wireless telecommunication networks coupled to the Internet.

By virtue of this dependency, we entrust Internet-enabled applications, programs, and connected devices with our most private communications and personal and financial details. Yet we read, almost on a daily basis, of hacks and compromises on a gargantuan scale, of the very systems we entrust with our private business and personal data.

The disclosures of Edward Snowden and others have increased public awareness about the need to be mindful of cyber security and cyber threats in our IT-centric world of smartphones, Internet, and Cloud-based services.

Businesses are faced with many of the same cyber security risks as individuals, but businesses are made to bear greater legal and financial responsibility in the event of a compromise.

Today, cyber security, including data protection, is a board-level critical business risk area. A major compromise of a corporate IT system may raise significant business continuity and business reputation risks, in addition to possible lawsuits by customers and actions by the government/regulators, such as investigations, penalties, and fines. Companies now find their risk management committees devoting more and more time to cyber security issues.

The cyber risk landscape is highly dynamic, making ongoing proactive prevention necessary but difficult. Moreover, it is very difficult for a business to keep a breach of its IT system private, irrespective of legal obligations or attempts to control public disclosure that a system has been hacked.

Worse still, the detection of a compromise or hack often happens many months or even years after the initial compromise. Clearly, dealing with cyber risks requires diligent attention. But given the dynamic nature of cyber risks, what areas should a business focus on when establishing a program of cyber security preparedness?

Cyber security preparedness necessarily involves much more than board supervision and risk management committee oversight. It also requires a review of what cyber security processes, structures, and mitigation measures government regulators expect in each of the jurisdictions where a company does business and/or where the relevant data resides. Going beyond legal issues, the review must also take account of practicalities, including costs, perceived risk, and objective reasonableness.

One key component of such a review is an assessment of vendor risk management, which has become even more important given the broad adoption of Cloud services. The review should include consideration of vendor policies, procedures, and contracts to ensure the sufficiency of security obligations and legal remedies to protect the company against a compromise by, or through, any of its vendors.

Cyber security risk assessment has also become a core component of due diligence, particularly in mergers and acquisitions. In addition to considering whether there are any ongoing regulatory investigations or enforcement actions relating to breaches or other compromises, a due diligence review should address whether the target company has critical data assets (e.g., personally identifying information of customers and/or credit card data) and whether the target has experienced data breaches, and if so, provide an explanation of the damage and how it was mitigated. It should also take account of the risk of future breaches, and more generally, whether the target's cyber security program is adequate using both industry benchmark standards as well as legal requirements.

For example, a cyber security program should include an incident response plan that is tested through tabletop exercises with senior management, technology representatives, and legal counsel, and it should be kept up to date, taking account of new threats that are identified. The incident response plan should be developed using multiple scenarios to realistically simulate potential incidents including Advanced Persistent Threat (APT) intrusions, data theft, insider attacks, and denial of service attacks. The plan must also take account of the type of business. For example, retailers should consider point-of-sale attack scenarios.

> "businesses are faced with many of the same cyber security risks as individuals, but businesses are made to bear greater legal and financial responsibility in the event of a compromise"

While important, detection is merely the first step. Businesses should also have in place policies and procedures for a proper response, providing for appropriate escalation within the organization's management structure, mitigation of risk, and preservation of forensic evidence once a compromise is discovered. It should also protect attorney-client privilege materials and the company's legal rights, in case lawsuits or government or regulatory investigations subsequently arise.

In today's world, companies need to take a proactive stance in dealing with cyber security. Companies' dependence on IT systems and Cloud-based services will only increase, and cyber security will continue to become ever more important. Companies must prepare for attacks from the inside as well as from outside third parties (including both criminally-motivated individuals as well as state-sponsored attacks).

Company executives, hand in hand with legal counsel and the technology team, must work together to continually evaluate a company's preparedness and develop and implement defense and mitigation strategies to prevent and limit damage due to cyber attacks.