A Cybersecurity Risk Assessment is the First Step to Managing your Compliance Burden

By: Larry Hershman, Managing Partner and Jeff Brenner, Partner and General Counsel

Traditional risk management is already a mission critical practice for businesses. Add to it the scourge of computer hackers tapping into IT systems via emails laden with malware or through insecure remote connections and it becomes a seemingly impossible task. Append those daily efforts to the increasing demands of state and federal regulators to be notified of potential breaches in almost real time and you get a business that may not survive the resulting costs and reputational damage.

The solution proactive businesses (and their counsel) are using to help identify how data flows through their companies, the risks it faces as it moves, and how to use that knowledge to rapidly respond the ever-changing data privacy/breach notification regulatory environment is a Cybersecurity Risk Assessment.

A Cybersecurity Risk Assessment focuses on the value of the information contained within a business's computers and the losses it may incur if that information is exposed, destroyed, stolen, or becomes otherwise inaccessible. The Assessment identifies and categorizes the critical electronic data in the business's possession or control, where that data is located, who has access to it, and the strength of the business's current IT systems and controls to protect it from harm. This catalog of information allows business leaders, risk officers and legal counsel to build, upgrade, and maintain systems, processes and protocols which will ultimately reduce the risk of a cyber incident, limit the legal, financial and reputational exposure should an incident occur, and enable the business to respond to regulatory notification requirements in an efficient and cost effective manner. This strategy ultimately aligns with the goals of state and federal data and privacy regulations and responsibilities.

A Cybersecurity Risk Assessment is often confused with protectionist tools like cybersecurity audits, vulnerability assessments, and penetration tests. Each tool is important, but they are not interchangeable nor do they address the business's IT architecture as a whole. These tools are designed to evaluate the strength or weakness of a particular piece of software (computer operating systems, programs, applications), or hardware (routers, firewalls), or business processes (data flow and usage), and the channels over which the business's information flows (third party vendors, cloud storage, email). The results these tools yield become part of the Cybersecurity Risk Assessment and impact how the business re-organizes itself, its processes, and its equipment to better protect its data and the value it represents.

New Regulations to Come:

The Office of the New Jersey Attorney General recently announced that it will be creating a new civil enforcement unit, known as the Data Privacy & Cybersecurity Section, to investigate data breaches impacting New Jersey residents and to enforce federal and state data privacy and cybersecurity laws. New Jersey's AG joins an expanding list of state AGs, including those of California, Connecticut, Indiana, Maryland, Massachusetts, New York, and North Carolina, who are dedicating more resources to data breach investigation and enforcement actions.

In 2017 the New York Department of Financial Services released Cybersecurity Regulation 23 NYCRR 500 (DFS 500), a set of regulations that places new cybersecurity requirements on all covered financial institutions. In addition, the NY state Attorney General has proposed the SHIELD ACT, which would place a legal responsibility on companies to adopt "reasonable" administrative, technical, and physical safeguards for sensitive data; the standards would apply to any business that holds sensitive data of New Yorkers, whether they do business in New York or not. The performance of a Cybersecurity Risk Assessment is a primary requirement for compliance with these regulations.

Pennsylvania is one of 24 states that requires customer notification, "without unreasonable delay," when a data breach affects more than 1,000 residents. Pennsylvania's attorney general is taking on a national role on data breaches in the midst of a wave of incidents impacting millions of Americans and Pennsylvanians. Attorney General Shapiro filed his office's first-ever lawsuit under Pennsylvania's Breach of Personal Information Notification Act against the ride-sharing company Uber based on a data breach impacting 600,000 Uber drivers in the United States – including 13,500 in Pennsylvania.

Performing a Cybersecurity Risk Assessment will not only improve the business's security posture, it will help align the organization with these, and other state and federal regulations and activities (e.g. Sarbanes Oxley, HIPAA Privacy, PCI) and the most recent addition, the international data transfer requirements of GDPR (General Data Protection Regulation). Knowing where the data is, what personally identifiable information it contains, who has access to it, and for how long, will not only put the organization in the most efficient compliance posture, it will greatly improve its incident response time.

To learn more about how Black Cipher Security can help improve your outcomes, visit our website at **www.blackcipher.com** or email **info@blackcipher.com.**