Primerus
The World's Finest Law Firms

"Avoid Being the Next Data Breach Headline: Lessons for In-House Counsel"

Thursday, June 11th, 2015 (4:00-5:15 p.m.)

Presented by:
Gerry Balboni – Krevolin & Horst – (Atlanta, GA)
Halsey Knapp – Krevolin & Horst – (Atlanta, GA)
Bernie Resser – Greenberg Glusker – (Los Angeles, CA)
Khizar Sheikh – Mandelbaum Salsburg – (Roseland, NJ)

Program Takeaways

1. Create interdisciplinary collaborative teams and communication protocols to address prevention and response: including Information Technology (especially Information Security), business unit heads, compliance, HR, PR/Investor Relations, General Counsel, and of course outside counsel – to assist with strategies for breach notification, regulatory investigations, and litigation.
2. Encrypt most sensitive data even within the firewall.
3. Add programs that identify use of company data by authorized users that is out of ordinary to detect hackers with stolen credentials called User Behavior Analytics or UBA
4. Due diligence to include vendors and portals for vendors; segmentation.
5. Manage fall-out with "managed transparency" "Be up front with regulators, consumers, employees, and shareholders and do that in a timely way." Zack Warren, "Data Breach 411: Are You Prepared?" Inside Counsel, March 30, 2015.
6. Include monthly IT security assessment with every monthly financial report.
7. Cyber Insurance.
8. Communication is key!
9. Train employees with fake phishing tests.
10. "My recommendation to those that had their information breached is the following: Sign-up for identity theft protection as this will alert you if someone has tried to open up a credit card in your name, which requires a SSN. Lastly, I would be very careful in opening up attachments or clicking on links within emails that claim to be coming from Anthem."
11. http://www.securityweek.com/feedback-friday-industry-reactions-anthem-data-breach
12. Why cybersecurity should be embraced by the law department and not sit within the IT department alone.
13. The key risks: hacktivists, organized criminals, government spying, and corporate insiders.
14. How in-house counsel can manage cyber-risk, starting with enterprise risk and then looking at specific aspects of risk: regulation, contracts, third parties, dispute resolution, cybersecurity, and policy and education, awareness and vigilance.

15. How to craft and test incident response plans.
16. The significant impact of a data breach make cybersecurity a business risk, not simply an IT risk. Strong executive and board support is critical to development of a culture of security to mitigate this business risk. Routine employee training reinforces this culture and is the first line of defense against "social engineering" attacks - such as phishing.
17. Periodically (at least annually) lead a review of the company's data security policy - Does the policy clearly define roles and responsibilities to identify, assess, and manage cybersecurity risks across the enterprise? Is the a process for identifying, classifying, and securing sensitive data? Are logs of file level access maintained? Is any surveillance of unusual file activity?
18. Periodically review (or develop) an incident response plan that addresses (a) information security (b) compliance, (c) public relations, (d) business continuity, (e) cyber insurance, and litigation. Does the Plan address damage assessment and containment? remediation? eradication? crisis managment? preservation of evidence? compliance with state (and perhaps federal) breach notification laws?
19. Before an incident - engage outside advisors - data forensics, IT security, public relations, and outside legal counsel.

[T]here are only two types of companies: those that have been hacked and those that will be."

Robert Mueller, Former FBI Director