10 Information Security Topics to Review With Your Board of Directors

With an increasing number of data breaches showing up in the headlines, your board of directors wants to know if and how your company is protected and what your role and strategy is in addressing these risks and exposures. To help you prepare for your next board meeting, we encourage you to consider the following topics to review with your board of directors on, at least, an annual basis.

1. **Key Overall Cyber Security Program Elements**—provide and talk-through your cyber security program plan, and identify any gaps that may need to be addressed insofar as how you're approaching the big-3 questions:
   i. What are our exposures?
   ii. Have we been breached?
   iii. Are we optimizing and running our infosec program properly?

2. **Risk-Based Approach to Security**—ensure that you and your board members understand the risks in your infosec and company profile and how you're tackling infosec with a risk-based approach (rather than simply putting up firewalls, for example, and driving a legacy "block-and-protect" approach to information security).

3. **Incident Detection**—discuss what tools and program approach you have in place to detect breaches; how will you know if there is or has been a breach and what information will be available to you about it?

4. **Vulnerability Testing and Exposure Validation**—provide your infosec point-of-view on understanding your exposure profile, particularly with respect to recognizing and validating those vulnerabilities and whether to hire a third party for retainer services or a penetration test.

5. **Incident Response Plan**—lay out your "disaster recovery" plan, considering who will be informed and involved when a breach occurs. This should include members of IT, InfoSec, Finance, Legal, Marketing, Investor Relations, HR, and your PR agency.

6. **Monetary Impact of a Breach**—ensure that you have ranges for what the impact would be from a financial perspective in the array of outcomes; this should include the loss of customer data, privileged information, legal fees, and more.

7. **Cyber Liability Insurance Coverage**—evaluate your cyber security coverage; how much $ coverage do you need/have and what have you decided to cover; what tools or third parties have you used to identify and evaluate those risks?

8. **InfoSec Org Structure**—we recommend that the Information Security team not report into IT but rather to the CFO, COO, or CEO; ensure that your board understands the benefits of why that's so and the alignment and good governance that it drives (e.g., having infosec report into IT is like having internal audit report into the controller).

9. **The Role of the CISO**—do you currently have a CISO on board, and if not, talk about the leadership of the infosec function both strategically and tactically.

10. **InfoSec Budget**—review your budget and identify what percentage should be allocated toward information security now and over time; you'll also want to discuss the divide between prevention-based tools, incident detection and response tools, and third party services.

Learn more about what your company can do to prepare for a breach and explore the range of solutions offered by Rapid7 at www.rapid7.com.

RAPID7