March 15, 2016

Safety In Numbers: Cybersecurity 101 for the IRO

Steven Shapiro

KRASNOW SAUNDERS KAPLAN & BENINATI LLP

1

Cybersecurity Threat Challenges

Cyber Threat Landscape

- Many actors/motives, but similar tools and techniques
- Shared/integrated domain – greater connectivity
- Accelerated speed of attack
- Attack surface is growing

Global Challenges

- Dependence on ICT
- Attribution
- "Wild West" – establishing norms of behavior; harmonization of legal regimes
- Awareness and education

Organizational Challenges

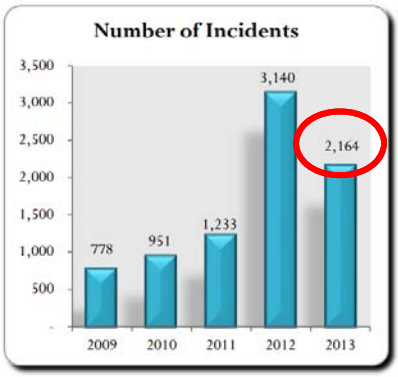
- Limited budgets, expertise and too many competing priorities
- Keeping pace with dynamic and sophisticated adversaries

No such thing as perfect security; incident response key aspect of legal and business risk management.

2

2

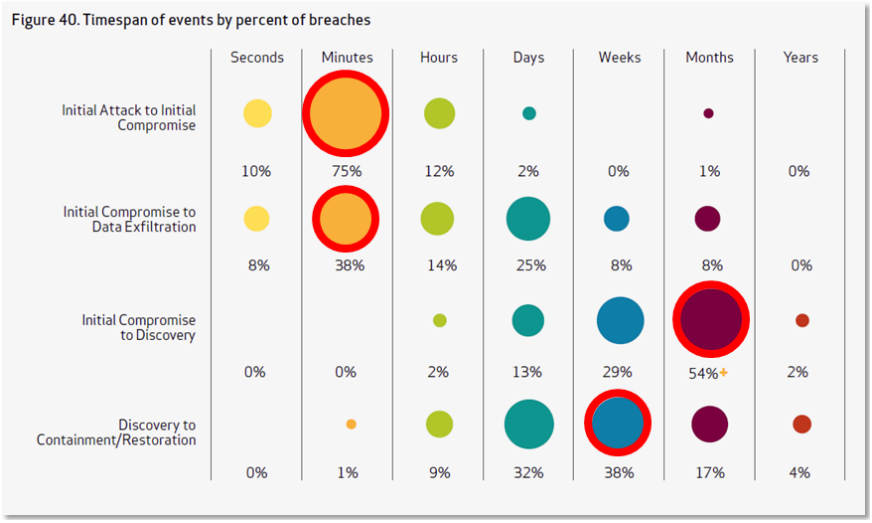
5 Year Trend



Verizon, "Data Breach Investigation Report"

3

Time to Impact vs. Time to Discover



Verizon, "Data Breach Investigation Report"

4

Cybersecurity is the No. 1 Concern of General Counsel and Directors

5

5

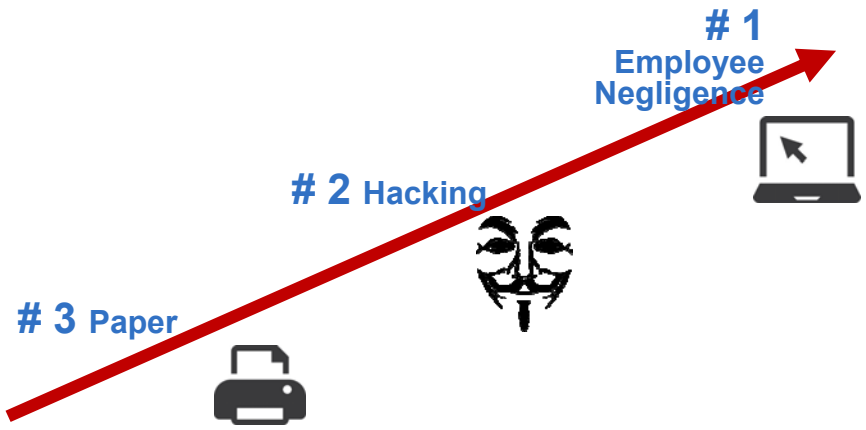
Corporate Governance

- A board may fulfill its duties and reduce the risk of liability for cybersecurity events in a number of key ways, including:
  - ensuring that the company has a plan to address a cybersecurity event that is communicated to appropriate company personnel;
  - making a good faith effort to become informed about cybersecurity risks and vulnerabilities and the implementation of strategies to protect the company's data, networks and infrastructure;
  - taking affirmative steps to assess and to monitor material aspects of the company's cybersecurity; and
  - seeking changes in policies and practices where warranted.

6

6

What's Your Biggest Exposure?



7

7

Does Insurance Cover Cyber Losses?

- *Yes, but:*
  - *It's not one policy.* Different types of insurance coverage in the company's portfolio might apply.
  - *It's not all covered*. Several areas of loss are difficult to quantify and insure, e.g. trade secrets or other intellectual property.
  - *The insurer might not pay*. Having an insurance policy is not the same things as having a claim paid.

8

8

Potential Sources of Protection

- Traditional insurance products
  - First-party property
  - Crime/employee dishonesty
  - Third party liability
  - Directors' and officers'/"management" liability
- Specialty "Cyber-Risk" or "Cybersecurity" insurance products
- "Other people's insurance"

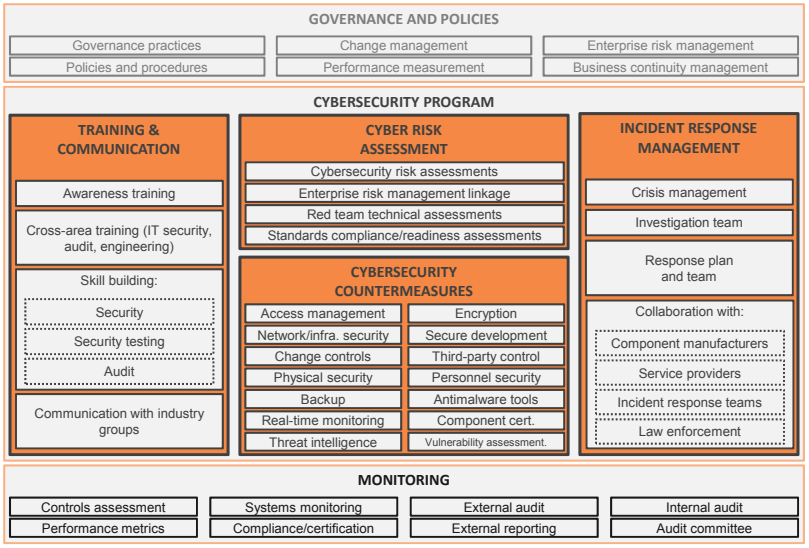
* * *

Carnegie Mellon 2012 Cylab Report: 58% of respondents (Forbes Global 2000) said the board did not review the organization's coverage for cyber related risks.

9

9

A robust cybersecurity program is critical



10

10

Cybersecurity Governance

Top Ten Recommendations for Cybersecurity Governance

1. Involve the board and senior management across departments.
2. Recruit management with IT and security/risk expertise.
3. Use board committees to oversee cyber issues. and set a reporting threshold for breaches.
4. Develop a comprehensive cybersecurity incident response plan.
5. Audit and test security measures on a regular basis.
6. Consider the cybersecurity policies of third party service providers (e.g., legal counsel and accountants).
7. Review insurance coverage for cyber-attacks or breaches.
8. Require cybersecurity training.
9. Review and update public disclosures regarding cybersecurity.
10. Consider the impact of security breaches on internal control over financial reporting.

11

11