A CISO's Journey
… from the Basement to the Boardroom

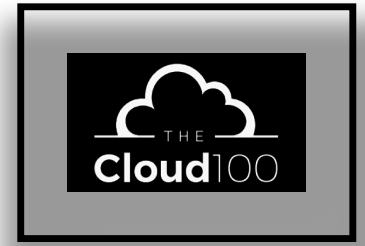
Craig Rosen, VP & Chief Information Security Officer, Presentation to ISSA: October 2016

APPDYNAMICS

A bit about me.

- **Current: VP & CISO, AppDynamics: 6 months**
  - SW/Tech: Application Performance Monitoring
  - HQ in San Francisco
  - Privately held, 1000 employees
  - Cloud and on-premise customer implementations

APPDYNAMICS
#9 in Forbes Cloud100



- **Current: Advisor, SafeBreach: 11 months**
  - SW/Tech: Security Automated Red-Teaming

- **Prior:**
  - VP & CSO, FireEye: 3 years
  - Security Director, Large Investor Owned Utility: 6 years
  - Security Consulting, Federal and Commercial: 12 years

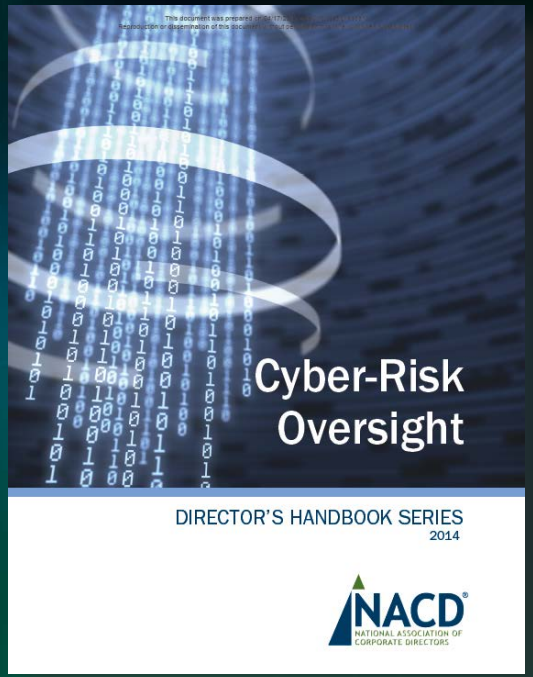
Moving from the basement to boardroom

- Two objectives for today's discussion

How did we get here?
(and why the opportunity is now)

Tips to get yourself prepped for the boardroom discussion.

“If a sophisticated attacker targets a company’s systems, they will ***almost certainly*** breach them.”



Breach inertia?

- Dec 2013: Target breach, 40M customers
  - Mar-May 2014: Target CIO and CEO resign
  - June 2014: 7 of 10 Board Director removals up for vote
  - Multiple shareholder derivative lawsuits filed against Target
  - Mar-Dec 2015: costs of approximately $290M to date
- 2014 victims: Home Depot, Neiman Marcus, Sony, JP Morgan, etc.
  - Sep 2015 shareholder derivative suit filed against Home Depot
- 2015 victims: OPM, Anthem, LastPass, Ashley Madison, IRS, etc.
  - July-Aug 2015: OPM Director and Ashley Madison CEO resign
- 2016 victims: Yahoo!, LinkedIn, Dropbox, Wendy's, IRS^{v2}, etc.

Is anyone [*really*] listening?

- June 2014: “Cyber Risks and the Boardroom”
  - Landmark speech by the SEC Commissioner
- June 2014: NACD’s Cyber-Risk Oversight handbook
  - 5 key principles Boards should adopt
- Jan 2015: ISSA Journal, Front Page!
- Oct 2015: NYSE releases 355-page publication
  - The Definitive Cybersecurity Guide for Directors and Officers
- Dec 2015: ‘Cybersecurity Disclosure Act of 2015’
  - Senate Bill regarding public disclosure about cybersecurity expertise on Boards (and lack thereof).

> “Boards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril.”
>
> *Commissioner Luis Aguilar*

2014 measures

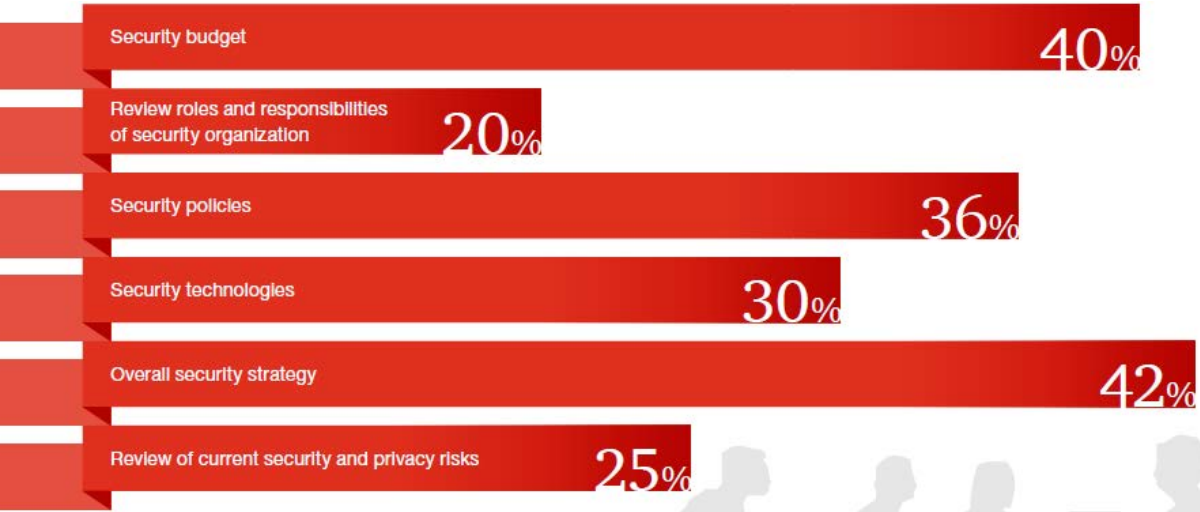


Figure 10

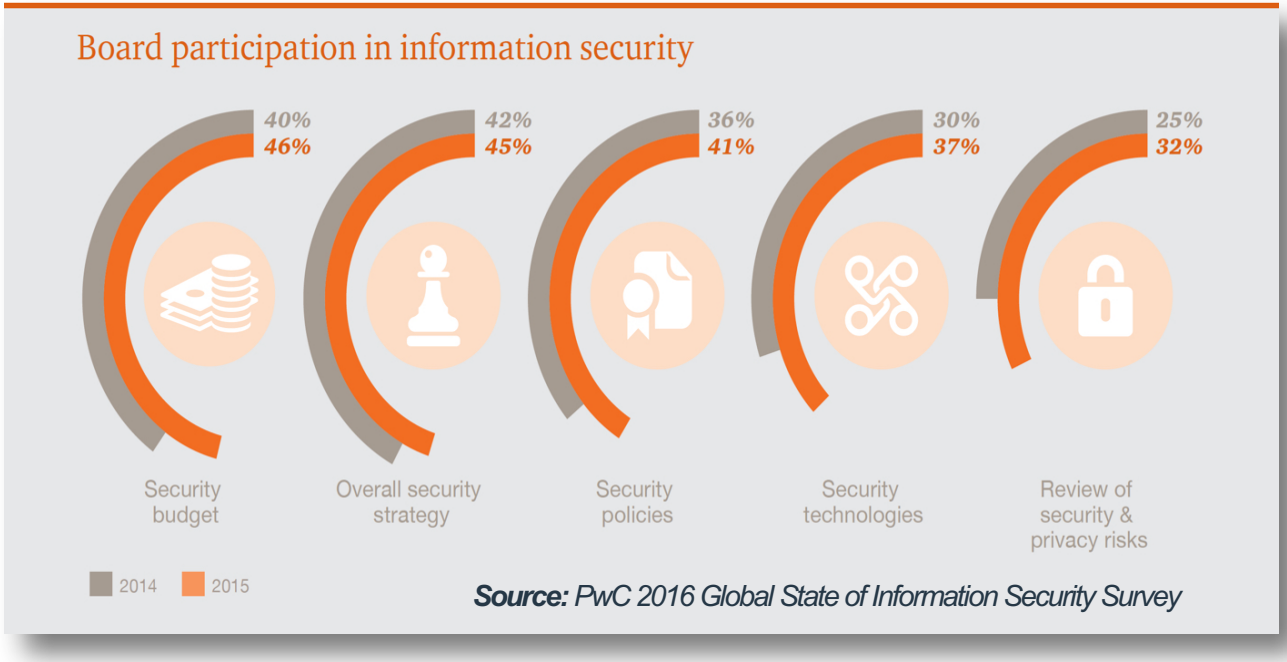
At most organizations, the Board of Directors does not participate in key information security activities.

Despite the high-profile security breaches in the past year, the Board of Directors is often not involved in critical initiatives such as security strategy, budget, and review of risks.

> *"It is incumbent upon the executive team to take ownership of cyber risk and ensure that the Board understands how the organization will defend against and respond to cyber risks."*
>
> *PwC 2015 GSISS Report*

Source: *PwC 2015 Global State of Information Security Survey*

One year later (2015) … opportunity knocks.



"Boards **appear to be listening** to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security."

PwC 2016 GSISS Report

Moving from the basement to boardroom

- Two objectives for today's discussion

Even if they don’t ask, answer.

1. Here’s what we are up against
2. Here’s what has happened
3. Here’s what *might* happen
4. Here’s what we’re doing about it
5. Here’s why our customers care

Even if they don’t ask, answer.

1. Here’s what we are up against
   - Show what assets and asset groups you are protecting
   - Show you understand your threats and adversaries
   - Show you understand the business impact/risk implications
   - Show you know how to put it into context, visually (“placemat”)

Even if they don’t ask, answer.

2. Here’s what has happened
   - Cover incidents, but review the ones that matter
   - Note the number of incidents since last meeting, regardless
   - Cover incident response efficiency: leverage metrics like speed of detection and response efforts
   - The “near miss”: consider raising what *hasn’t* happened

Even if they don't ask, answer.

3. Here's what *might* happen
   - Be clear that things will continue to happen - but avoid FUD
   - Anchor them on *your* measuring stick
   - Show what risks you definitively know by asset group
     - Cover vulnerabilities, but indirectly as risks
   - Show "control coverage" and what you don't *yet* know
     - Explain how risks will change
   - Recommend a risk threshold … then listen

Even if they don’t ask, answer.

4. Here’s what we’re doing about it
   - Discuss your current controls and their effectiveness
   - Show your initiatives by priority based on your strategy
   - Show progress by quarter
   - Discuss functional maturity and how improving it will help more *efficiently* manage the risks
   - Recommend a maturity goal in 12-24 months

Even if they don’t ask, answer.

7. Here’s why our customers care
   - Show a metric that ties in customer concern
   - Discuss the pressures customers are dealing with, in their verticals
   - Commit to helping relieve that pressure

Putting it all together.

- Inaugural meeting, 45 minutes, set stage:
  - Establish the narrative on the 5 previous areas: “placemat”, risk, metrics, maturity, thresholds
  - Discuss strategy for risk management
  - Setup quarterly expectations
- Quarterly meeting: 20 minutes, 4 slides:
  - Slide 1: Last QTR accomplishments (in priority)
  - Slide 2: Next QTR plans (in priority)
  - Slide 3: Obstacles to accomplishing goals
  - Slide 4: Risk metrics
- Lather, rinse, repeat.

In conclusion…

Thank You