CISO Survival Guide: How to thrive in the C-Suite & Boardroom

Chris Wysopal
Co-founder, CTO & CISO
Veracode

October 20, 2015
Chris Wysopal, CTO, CISO & Co-Founder

• 15+ years focused solely on application security
• One of the original security researchers from mid 90’s. Was part of hacker think tank, The L0pht.
• Founded Veracode to build automated application security testing
• My son now keeps me busy installing Minecraft mods.
Agenda

• Boards are concerned with Cybersecurity
• NYSE Survey Results
• Communicating today’s risks to the board
• Communicating security posture to the board
Why are boards concerned about security?
Why are boards concerned about security?

WITH INNOVATION COMES RISK

Security incidents grow 66% CAGR
The total number of security incidents detected showed an increase of 48% over 2013.

Bank Hackers Steal Millions via Malware

Russian Hackers Amass Over a Billion Internet Passwords

Community Health Systems breach could cost up to $150 million

Cybercriminals Had Banner Year in 2014, Symantec Report Says

Attacker exploit zero-day flaw in popular WordPress plug-in

Researchers hijack teleoperated surgical robot: Remote surgery hacking threats

Premera Blue Cross Breach Exposes Financial, Medical Records
Cybersecurity in the boardroom survey

- 200 Board Members
- 6 Industries
- 69% Multiple Boards
NYSE Survey Results
80% of respondents discuss cybersecurity at most or all boardroom meetings

Directors lack confidence in their companies’ ability to thwart an attack and are increasingly holding the CEO and, in some cases, the entire executive team responsible.

ARE BOARD MEMBERS CONFIDENT IN THE CYBERSECURITY OF THEIR COMPANIES?

66% of board members are less than confident that their companies are properly secured against cyberattacks

WHAT ARE BOARD MEMBERS’ BIGGEST FEARS?

1. BRAND DAMAGE
2. BREACH COSTS
3. CORPORATE ESPIONAGE
Nearly two-thirds of respondents prefer cybersecurity info to be presented as risk metrics or high-level strategy descriptions.

CISOs should speak to the board in terms directors understand, such as by using analogies and talking about breaches in similar industries.

While the pressure resulting from a breach might have shifted from the CISO to the CEO, in terms of accountability to the board, survey results show the CISO can take practical steps to become a more effective leader.

The Ideal CISO Builds Upon Technical Skills
More than 70% indicated they have significant concerns about risk from third-party software.

One board member commented on an “inability to know whether customers and suppliers who use our systems have adequately secured their own access points.”
A CISO's Perspective on Talking to the Board About Cybersecurity
The CISO’s role is changing

- No longer a back office technology expert
- Business leader that is strategic
- Needs to communicate across company leadership: IT, Legal, Risk, LOB, PR
- More visible role
What is the Board’s Role?

The Board is not the executive. They don’t make decisions.

- Represent shareholder interest
- Appoint executive management
- Support exec in strategy development and implementation
- Test quality of execs implementation
- Place company direction and performance in context
NACD Guidance on Cybersecurity

- Enterprise wide risk management issue
- Legal implications
- Needs regular and adequate time on the agenda
- Need specific plans associated with each risk approach
Meeting Board Expectations

• No longer just an audit function
• Discussion on risk and risk posture
• They want to know what are the odds our company with experience a damaging security breach and what are we doing to prevent that
• Answering at right level can gain confidence in your security agenda
• Breach readiness and breach response are hot discussion topics
Communicating with the Board

Build Trust

• You will only get 5-15 minutes devoted to the cybersecurity topic
• Prepare an appendix for anything beyond a few key indicators
• Do not use acronyms - think “denial of service” not DDoS
• Use visuals not text
• Use numbers, especially dollars if possible such as losses from public data breaches
• Use analogies
Communicating with the Board

• Ask the question, “What do you want to get out of your information security program?”

• Concepts to get across:
  - There is no sure thing as a breach free organization
  - Cyber security is a company wide responsibility: IT, Legal, Risk, LOB, PR must become involved
  - Cyber security needs to be thought of as a long term strategy of survival of the brand
Communicating Today’s Risks

- Breaches in similar industries
- Key trends in successful attacks
- Who is out to attack OUR company
Communicate Risk Posture

- Describe top 5 cyber risks the company faces and the risk indicators that signal the company’s level of exposure to them
- Identify if risk indicators are trending up, down or remaining flat
- Explain how the company is managing security risks and keeping them within acceptable limits
- How do we compare to peers?
- Use industry benchmarks if available
Q&A

Chris Wysopal
cwysopal@veracode.com, @WeldPond