SO YOU JUST GOT INVITED TO BRIEF THE BOARD OF DIRECTORS ON SECURITY

Alan Paller
The SANS Institute
paller@sans.org

SEPTEMBER 2016, DALLAS, TX
Copyright 2016. SANS Institute
The CIO emails the CISO saying that Board of Directors is meeting next week; they want to be briefed on cybersecurity. You, the CISO, are on the agenda.

• A big opportunity? Perhaps.
• A high risk moment? Most certainly.
1. Because security programs benefit from top level support

- Senior management support enhances budgets and provides added weight when you want to implement important changes.
2. First impressions last a long time:

• Every member of the audience evaluates you almost continually.

• They remember.

• Each new encounter allows them only to adjust their perception.

This is an audience in which the first impression you make is likely to matter for your career.
Shellye Archambeau:

Member of the Board of Directors of
• Verizon
• Arbitron
• Nordstrom

CEO of MetricStream

Answers the questions:

What does the board want to hear in your briefing, and what defines success for you?
1. What is the big goal? What do you want them to do/feel/say after the meeting? (S1 to 0:58)

2. What should you leave out? (S2 to 2:22)

3. Are there best ways to present data – a standard for comparison? (S3 to 0:40)

4. Is this a great opportunity to increase our budget so we can handle the increasing risk? (S4 to 1:54)
What will you learn today?

- The key error that turns senior level audiences against security speakers
- What to consider leaving out
- The most important things to include and why
- Examples you can use as models
EXAMPLES OF BAD SLIDES ACTUALLY USED IN A FEDERAL EXECUTIVE BOARD BRIEFING
“The arrogance of that guy was something – nothing but jargon – and nothing showing he had a clue how to manage a hundred million dollar program.”

The bottom line: The woman who took his job called me last week.
Seasoned leaders approach security asking three questions:

1. What do we need to do to be secure?
2. How much is enough?
3. Whom can I trust to answer the first two questions?
HOW ABOUT THIS APPROACH?

“We are very fortunate that we have not been breached yet.”
“We are very fortunate that we have not been breached yet.”

Chairman of the House Intelligence Committee:

“There are two kinds of organizations. Those that have been hacked, and those that have been hacked but don’t know it yet.”
Approaches that have worked
Four CISOs who found effective paths
CISO 1: BOARD BRIEFING

Validated metrics of software security

Plus: (1) FBI Director to validate the immediacy of the risk and (2) CISO of a well known industry leader as a benchmark
CISO 2: Top Management Update

Continuous quarterly gap analysis vs the 20 Critical Controls

Plus: Continuous: (1) Mean time to Detect Incidents” and “Mean time to Contain Incidents and (2) 4 key automated vulnerability metrics – rolled up quarterly
90% risk reduction over 12 months
INTERLUDE: WHY DID THE CRITICAL CONTROLS WORK?
To be credible to management, metrics must be “authoritative and important and reliably measured”

How can you prove your metrics are authoritative and important (and reliably measured)?

The big idea:

“Offense informs defense!”
Who understands offense?

- NSA Red Teams
- NSA Blue Teams
- DoD Cyber Crime Center (DC3)
- US-CERT
- Top Commercial Pen Testers
- Top Forensics Teams
- JTF-GNO
- Air Force OSI
- Army Research Lab.
- Dept. of Energy National Laboratories
  - Sandia
  - Los Alamos

Would they be willing to combine their knowledge of attacks and offense to define the most important defensive investments CIOs must make to block all known attacks?
The Result: Twenty Critical Controls
Consensus Audit Guidelines (CAG)

• The twenty key controls
  1. 15 subject to automation: examples
  2. 5 that are important but cannot be easily automated
1. They define the highest priorities – what needs to be done, now!
   
   *That answers question 1:*
   
   “What do we need to do?”
   
   *and part of question 2:*
   
   “How much is enough?”

2. They are based on the consensus of proven experts who understand offense.
   
   *That helps answer question 3:*
   
   “Whom can I trust?”
Let’s start with the results:

• The Chairman of the Board told the CIO: “That’s the first time a security person has made sense.”

• And then he made the CISO’s budget “base” meaning it is funded automatically just like emergency power line repairs.
20 Critical Security Controls

Protection From the Most Likely Attack Vectors
Sample Red/Yellow/Green Metric

Prevention

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4) Continuous Vulnerability Assessment and Remediation
5) Malware Defense

Detection and Response

6) Application Software Security
7) Wireless Device Control
8) Data Recovery Capability
9) Security Skills Assessment and Appropriate Training to Fill Gaps
10) Secure Configuration of Devices such as Firewalls, Routers, and Switches

Identity, Access, Governance and Architecture

11) Limitation and Control of Network Ports, Protocols and Services
12) Controlled Use of Administrative Privileges
13) Boundary Defense
14) Maintenance, Monitoring and Analysis of Audit Logs
15) Controlled Access Based on Need to Know
16) Account Monitoring and Control
17) Data Loss Prevention
18) Incident Response Capability
19) Secure Network Engineering
20) Penetration Tests and Red Team Exercises
ONE MORE BENEFIT FROM USING THE VALIDATED CRITICAL CONTROLS

Auditor Buy-in
1. A solid answer for: What do we need to do?
   - Highest priority actions (the critical controls)
   - Validated source

2. A reasonable answer for: How much is enough?
   - Benchmarks from a provably high quality group.
   - Detailed, budgeted, scheduled plan to fill gaps (3 year)
   - Quarterly monitoring of automated, reliable measures of progress

- The answer to: Whom can I trust? will be
  - You! if you can do 1 and 2.
SUMMARY

• CISO’s perspective doesn’t necessarily match the Board of Directors’ perspective
  - What do I need to do? How much is enough? Whom can I trust to answer those questions?

• What seems to work:
  - Externally validated, prioritized framework (the critical controls) with a 3-year plan
  - Continuously showing improvement in important metric
QUESTIONS

apaller@sans.org