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

Alan Paller
The SANS Institute
paller@sans.org

February 2016 Orlando, FL
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. Because 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.
3. Because making cybersecurity presentations interesting and persuasive for non-technical managers is very, very hard.
Because perspective matters

1. Their perspective is nearly always different from the CISO’s perspective

2. It’s tough to change perspectives
The key error

Using your perspective rather than theirs – let’s look at two examples
WITH BAD SLIDES, HOW DID HE DO?
“The arrogance of that guy was something – nothing but jargon – and nothing showing he had a clue how to manage a multi-million dollar program.”
“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.”
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?
APPROACHES THAT HAVE WORKED

Four CISOs who found effective paths
CISO 1: 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

Quarterly Scoring Heat Map *

Level

Control Category

Compliant
Compliant in spirit of control
Work in progress towards compliance
Not appropriate for our culture
Gap with no current plan to correct

* Mock Data
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
20) Penetration Tests and Red Team Exercises

-Detection and Response
19) Secure Network Engineering
18) Incident Response Capability

-Identity, Access, Governance and Architecture
1) Inventory of Authorized and Unauthorized Software
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
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
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 priority – what needs to be done first

2. That answers question 1: “What do we need to do?”

3. Consensus of proven experts who understand offense

4. That supports answer to question 3: “Whom can I trust?”
ONE MORE BENEFIT FROM USING THE VALIDATED CRITICAL CONTROLS

Auditor Buy-in
CISO 3: 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 4: REPORTING TO CABINET, SECRETARY AND CONGRESS

90% risk reduction over 12 months

<table>
<thead>
<tr>
<th>CAG ID</th>
<th>Consensus Audit Guideline</th>
<th>NIST-800-53</th>
<th>US CERT Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory of authorized and unauthorized hardware</td>
<td>CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9</td>
<td>+ 6 %</td>
</tr>
<tr>
<td>2</td>
<td>Inventory of authorized and unauthorized software</td>
<td>CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7</td>
<td>+ 22 %</td>
</tr>
<tr>
<td>5</td>
<td>Boundary Defense</td>
<td>AC-17, RA-5, SC-7, SI-4</td>
<td>+ 7 %</td>
</tr>
<tr>
<td>9</td>
<td>Controlled access based on need to know</td>
<td>AC-1, AC-2, AC-3, AC-6, AC-13</td>
<td>1 %</td>
</tr>
</tbody>
</table>

Legend:
- **Red**: Domestic Sites
- **Blue**: Foreign Sites

89% Reduction
90% Reduction
SUMMARY OF WHAT TO INCLUDE

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.
EXTRA TIPS FOR BETTER RESULTS FROM YOUR PRESENTATIONS
• Starting into the core of your presentation before you have proven that the audience has ‘bought’ the problem you are there to solve.
How do you gently remind them why they are there?

The right story
• No speaker’s tool is more powerful - especially for technologists
• Use them to demonstrate why the problem matters
• Use them to prove the solution works
• Use them to counter objections
• Use them to change decision criteria
Effective Stories

- A problem that was important and damaging that was solved or at least addressed
- Includes a great deal of color about the problem (quotes from execs, numbers, etc.)
- Accurate, understated
- Provable (name used with permission)
• Stories that ends with thair saying “Oh”

• The best stories show an attack against *your own organization* and substantial cost/damage

• The “Oh” leaves the listener with no options other than asking “What do we need to do to defend ourselves against that?”
HANDLING QUESTIONS
HANDLING QUESTIONS

- Your moment to shine
- Questions belong to the audience
- Maintain authority
- Show you care
Really tough questions

- Can't hurt you, but you can hurt yourself:
  - Stop, take a step back
  - Look elsewhere
  - Restate
  - Answer the restated question
  - Ask for the next question
THE REALLY EASY QUESTION

• Take your time
• Give them the right answer
• Use it to reinforce your key point
• Do not say “I’ll get back to you”

• Take out a sheet of paper, ask for the person’s name and number, and write down the question.

• Ask whether anyone else also wants an answer to that one and pass the paper around.

• Before you leave ask, “Who has the sheet with the question on it?”

• Find the answer and send it out!
• CISO’s perspective doesn’t necessarily match the Board’s perspective (What do I need to do? How much is enough? Whom can I trust to answer those questions?)

• What works: Externally validated, prioritized framework (the critical controls) with a 3-year plan

• The right story can move mountains

• Even the toughest question cannot hurt you

• Want a copy: Email apaller@sans.org include your evaluation of the talk – its value for you and any suggested improvements
QUESTIONS

apaller@sans.org