

CISO Hot Topic: Communicating to and Influencing CEOs and Boards of Directors: What Works and What to Avoid

John Pescatore, SANS
Alan Paller, SANS
Steve Martin, CISO Cisco

Obligatory Agenda Slide

- Housekeeping info
- Here's what we will do
 - **18:15 – 19:00 CISO View** – Steve Martino
 - **19:00 – 19:30 Meaningful Metrics** – John Pescatore
 - **19:30 – 20:15 Communicating to Impact** – Alan Paller

Measuring the Right Things – Having Something Business Relevant to Say to the Board

John Pescatore, SANS



Characteristics of Cybersecurity Success

- Understand vulnerabilities and threats – table stakes
- Know demands of particular industry/vertical/organization
- Balancing demands
 - Reduce threat impact to business
 - Reduce security impact to business
- Ability to effectively communicate and drive action
 - Within the team
 - Across the organization
 - Upwards
- **Almost invariably, the organizations with the least cyber incident impact have the strongest CISOs and security teams.**

Communicating With Impact to Boards/CEOs

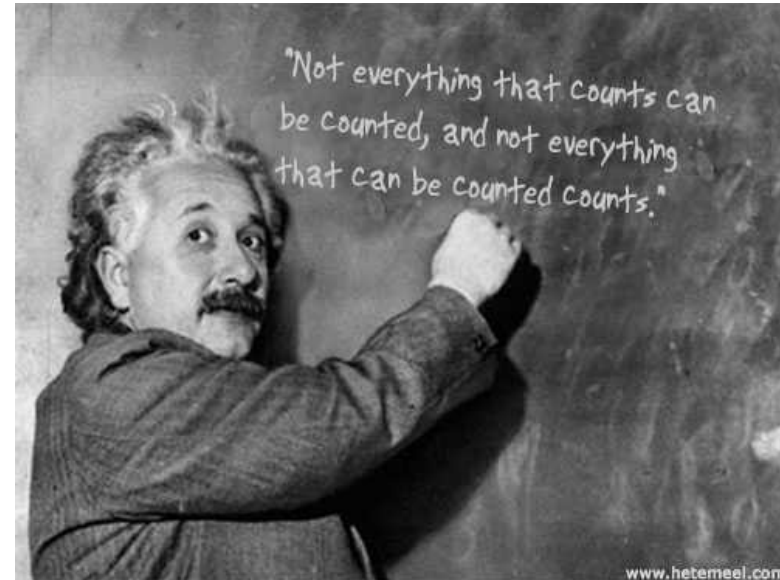


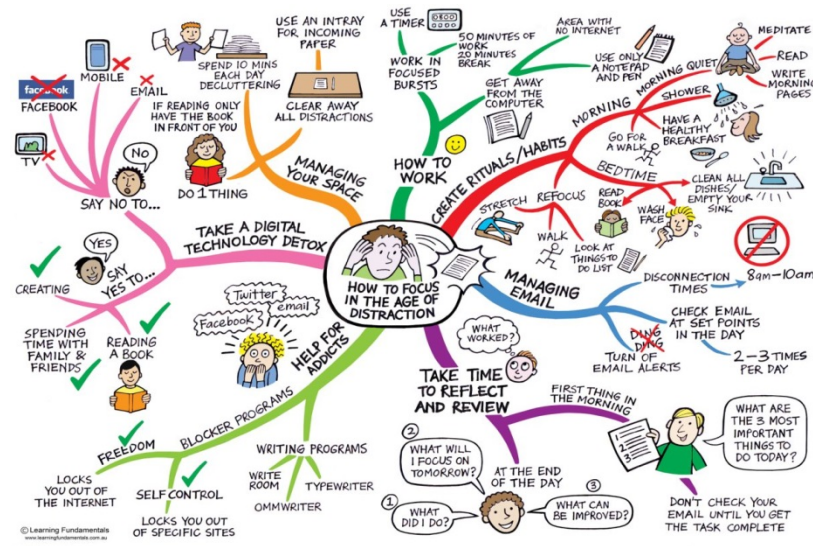
- Comments back from Board Members
 - “CISOs are great on ‘blood in the streets,’ weak on strategy to avoid it.”
 - “CISOs don’t speak our language – and seem to speak a different language each month.”
 - “The Board is strategic, not tactical” (Not an ATM machine...)
- **Metrics, prioritization, consistency, impact**

Avoiding the same old noise...



VS



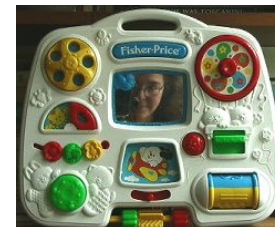
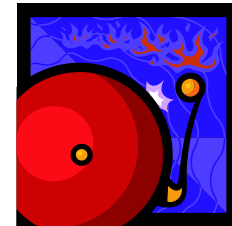


Focus on protecting the business first
 Effectively **and** efficiently **and** quickly
 Make sure the solution isn't worse than the problem
 Business benefits, not security features

Is it Safe Enough for Us to Self-insure?

Useful Security Metrics Can:

- Drive change
 - Increase efficiency
 - Increase effectiveness
- Give Warning
 - Action Required
 - Investment Required
- Demonstrate Value
 - Compete for funds
 - Motivate workforce
- Give the clueless a busy box



Delivering Security Efficiency and Effectiveness

Efficiency

- Decrease the cost of dealing with known threats
- Decrease the impact of residual risks
- Decrease the cost of demonstrating compliance
- Reduce business damage due to security failures
- Maintaining level of protection with less EBITDA impact

Effectiveness

- Increase the speed of dealing with a new threat or technology
- Decrease the time required to secure a new business application, partner, supplier
- Reducing incident cost
 - Less down time
 - Fewer customer defections
- Security as a competitive business factor

Sources of Examples



RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-107R

CHANGE
Challenge today's security thinking

**News Flash: Some Things
Actually Do Work in Security!!!**

John Pescatore
Director, Emerging Security Trends
SANS Institute
[@John_Pescatore](#)


#RSAC



Some Real World Examples


- **Healthcare** – BSIMM increase in secure app dev life cycle **reduced time to market for new app by 30% and reduced software development costs by 15%**
- **Higher Ed** - Intrusion Detection Rate **increased 46%**, corrective actions costs **decreased 35%**
- **Financial** – reduced PC reimaging due to malware from **4 per week to 1 every 3 months**, and will enable the use free of AV on desktops
- **Services** – firewall policy management tools enabled existing staff to **reduced new connectivity approval from 2 weeks to 1 day.**

Making a Difference Communicating Upwards




Parting Thoughts

- Remember Job #1
- Do Your Homework
- Metrics Matter
- The BoD Is Not an ATM
- Never Surprise Your ELT In Front of the BoD



22



Kim L. Jones CISM, CISSP

Source: Kim Jones, Vantiv CISO at SANS Scottsdale AZ CISO Hot Topics Session

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

Alan Paller
The SANS Institute
paller@sans.org

JUNE 2016, WASHINGTON, DC
Copyright 2016. SANS Institute

THE SITUATION

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.**

WHY DOES THIS MATTER?

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.**

WHY DOES THIS MATTER?

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.

IN THEIR OWN WORDS



Member of three Boards of Directors:

- 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?

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
- One extra tip for building trust

**EXAMPLES OF BAD
SLIDES ACTUALLY USED
IN A FEDERAL
EXECUTIVE BOARD
BRIEFING**

HOW DID HE DO?

- **Authority**
- **Energy**
- **Awareness**



...but Let's Be Honest: We Only Have Ourselves to Blame for Much of This



- **Haste to Jump on the Compliance Bandwagon**
- **Inability to Quantify Risk**
- **We (still) Suck at Metrics**
- **Communication Skills Can Be Lacking**
 - **“Pizza Boys” still abound (and are still necessary! But...)**

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 hundred million dollar program.”

HOW ABOUT THIS APPROACH?

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

HOW ABOUT THIS APPROACH?

“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.”

WHAT WENT WRONG? THE WRONG PERSPECTIVE

Seasoned leaders approach security asking three questions:

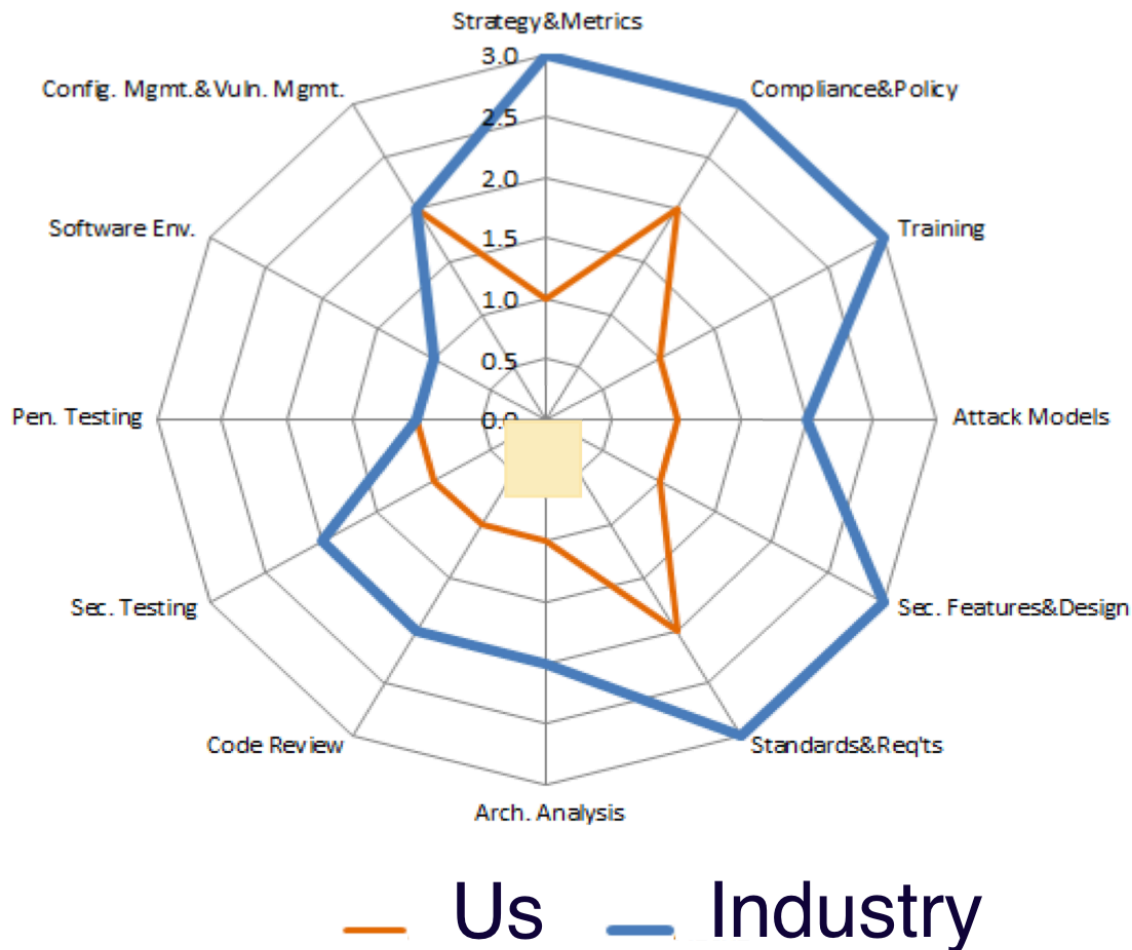
- 1. What do we need to do to be secure?**
- 2. How much is enough?**
- 3. Whom can I trust to answer the first two questions?**

APPROACHES THAT HAVE WORKED

**Four CISOs who found
effective paths**

CISO 1: BOARD BRIEFING

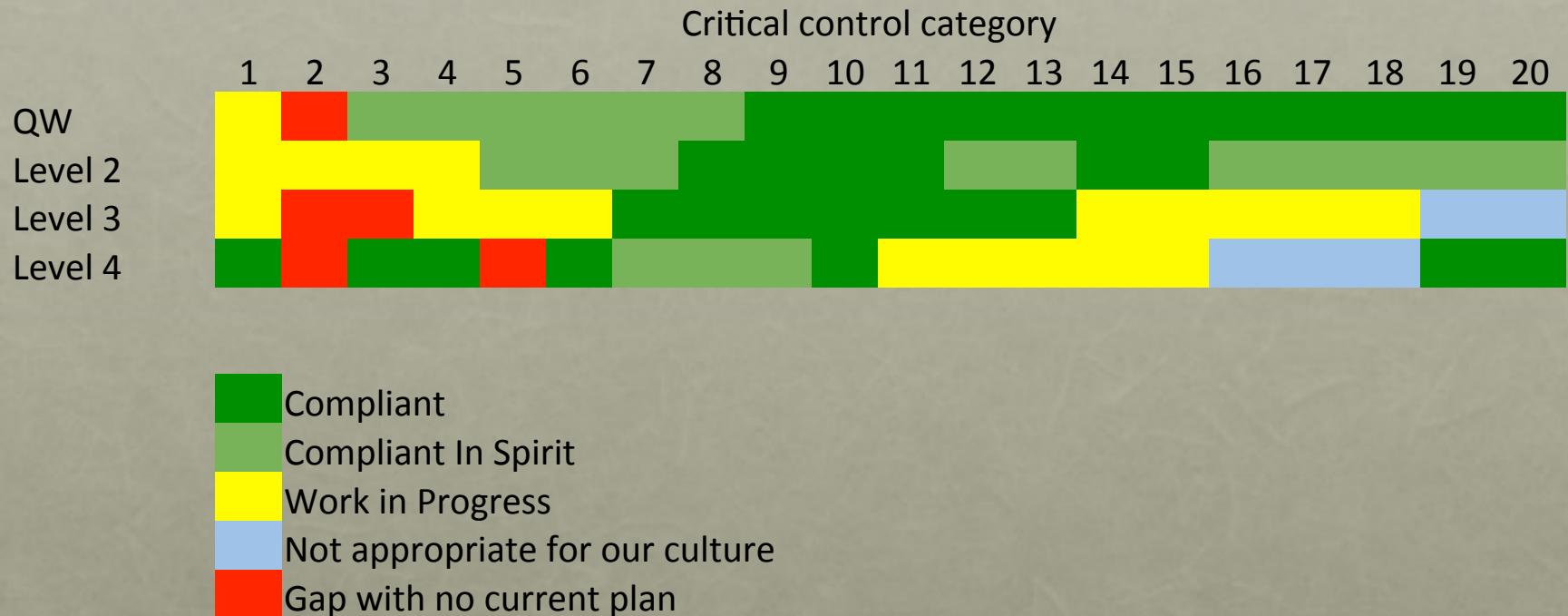
Validated metrics of software security



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

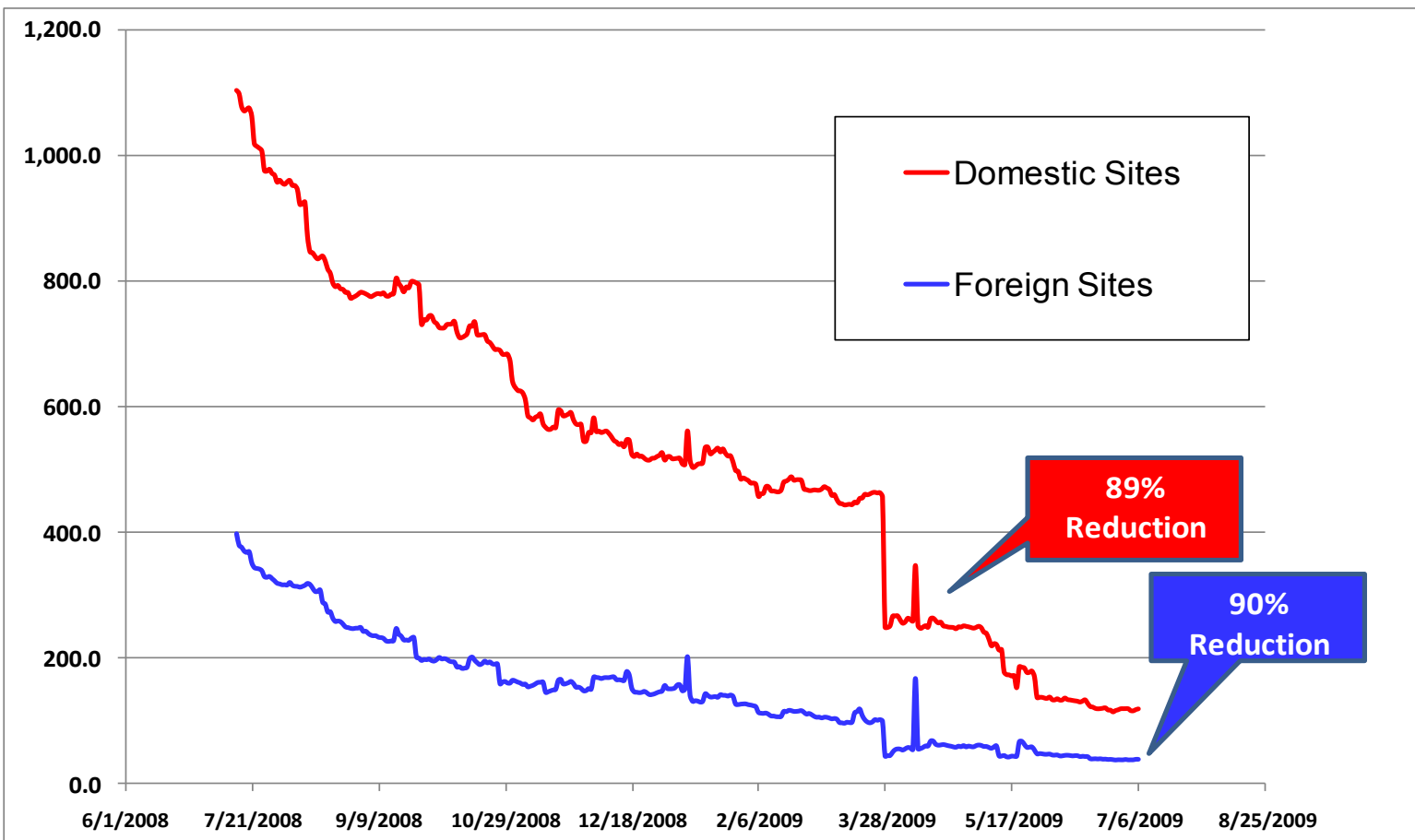


Plus: Continuous: (1) Mean time to Detect Incidents” and “Mean time to Contain Incidents and (2) 4 key automated vulnerability metrics – rolled up quarterly



CISO 3: Reporting to Cabinet Secretary and Congress

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**

WHY THE CRITICAL CONTROLS WORK

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?”

CISO 4: MAJOR UTILITY

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.**

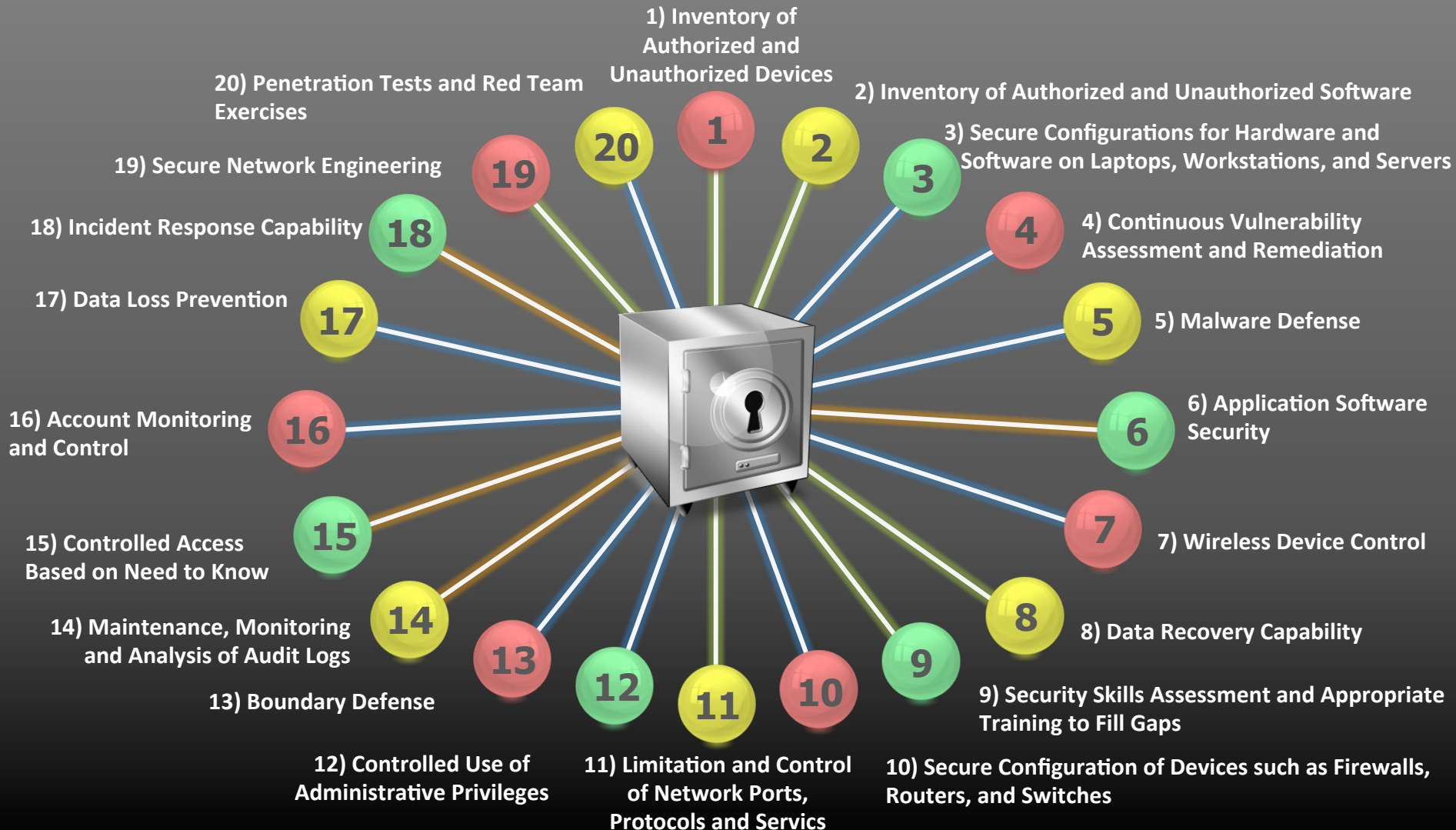
20 Critical Security Controls

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

-Prevention

-Detection and Response

-Identity, Access, Governance and Architecture



**ONE MORE BENEFIT
FROM USING THE
VALIDATED CRITICAL
CONTROLS**

Auditor Buy-in

SUMMARY; WHAT TO INCLUDE

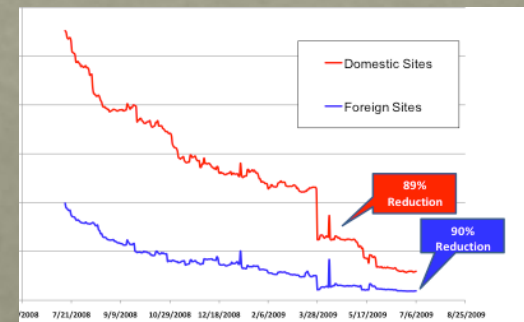
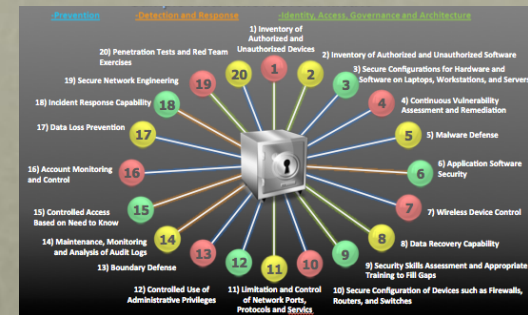
1. A solid answer for: What do we need to do?
 - Highest priority actions (the critical controls)
 - Validated source
2. A reasonable answer for: How much is enough?
 - Benchmarks from a provably high quality group.
 - Detailed, budgeted, scheduled plan to fill gaps (3 year)
 - Quarterly monitoring of automated, reliable measures of progress
- The the answer to: Whom can I trust? will be
 - You if you can do 1 and 2.

Bonus chance to gain trust: handling a question for which you “don’t know the answer”

- 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 for the sheet with the question on it?
- *Find the answer and send it out!*

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

When You Get Back to Work

- Make sure you are collecting the right security metrics so you can demonstrate value, improvement, danger.
- Take advantage of any transitions coming:
 - Moving to Windows 10, cloud services, mobile apps, agile dev, etc.
 - M&A, re-org, new C-level management.
 - Audit results
- Prioritize by business impact – shoot for a near term win.
- Change something!
- Communicate upwards
 - Successes
 - Strategic Obstacles
 - Recommendations

Resources

- SANS What Works: <https://www.sans.org/critical-security-controls/case-studies>
- SANS NetSec: <https://www.sans.org/event/network-security-2016>
- Questions: q@sans.org
- jpecatore@sans.org
- @John_Pescatore

By three methods we may learn Wisdom:

1.By reflection, which is noblest

2.By imitation, which is easiest

3.By experience, which is the bitterest



Confucius