Cyber Risk — What it Actually Means and How to Ignore the Buzz

Gal Shpantzer

Professional Strategies – S33

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

About Your Speaker

- Sr. Security Advisor, EnergySec
- Contributing Analyst, Securosis
- Consultant to EAmmune
- 12+ yrs. Infosec
- Infosec Burnout Study, SANS Newsbites
- NIST Smart Grid Privacy, DoE ES-C2M2
- Prior: Physical security, VIP Protection
- Full disclosure: Consult with some vendors

Overview

1. “Become the hunter”
2. Cybersecurity Elevation
3. The Swiss Cheese Effect … FUD in Context
4. Real or FUD (Fear, Uncertainty, Doubt)?
5. “What Can an Auditor Do to Help Security?”

What We'll Cover: FUD

- Stuxnet, Wikileaks, Snowden: Relevance?
- Appropriate paranoia: who & why?
- Protect which assets? Misplaced audit priorities
- Wheat field or bonsai tree?
- Checklists & HR?
- AV vs. White-listing: auditors & security
  PCI/NERC-CIP

1. Become the Hunter

“It’s natural for members of a technology-centric industry to see technology as the solution to security problems. In a field dominated by engineers, one can often perceive engineering methods as the answer to threats that try to steal, manipulate, or degrade information resources.

- Richard Bejtlich

Unfortunately, threats do not behave like forces of nature. No equation can govern a threat's behavior, and threats routinely innovate in order to evade and disrupt defensive measures. Security and IT managers are slowly realizing that technology-centric defense is too easily defeated by threats of all types."

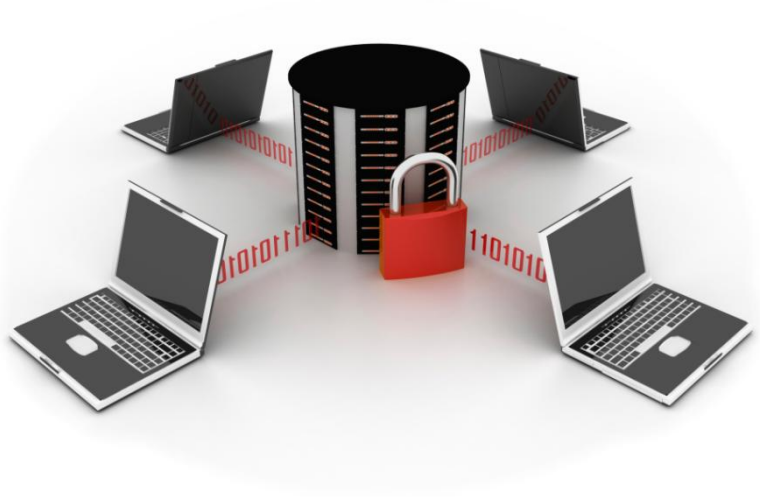
- Richard Bejtlich

Know What "They" Want (A)

- "It's nothing personal, it's just business."
- Disk space (FermiLab)
- Processing power (BitCoins)
- Bandwidth (DDoS)

Know What "They" Want (B)

- Information (advantage/embarrassment)
- Soft targets: business partners and law firms…
- Destruction (overt pain)
- Money (Direct via ACH)
- Money (indirect via PII, CC#, etc.)



2. Cybersecurity Elevation

Cybersecurity Elevation

- Increased Publicity
  - Hacktivists
  - APT1 Report
  - Zombie baby monitors
  - Cloud & mobile/apps
  - Stealth marketing & PR
- Increased Regulation
  - HIPAA, PCI, SOX
  - CA SB 1386 variants
  - Privacy

Notable Ongoing Failures

VA laptop, 2006 - VA OIG report, 2012

"As of July 2012, OIT had installed and activated only about 65,000 (16 percent) of the total 400,000 licenses procured. This was due to OIT's poor planning and inadequate management…

As a result, 84 percent of the total 400,000 licenses procured, totaling about $5.1 million in questioned costs, remain unused as of the end of fiscal year 2012."

Online Banking Heists

- Ski-mask behind a keyboard
- Bankrupt by a one-time heist
- Non-FDIC business checking accounts
- Compromised clients, not bank

KrebsonSecurity
In-depth security news and investigation

Target: Small Businesses

Other / Target: Small Businesses — 56 Comments

7 AUG 13

$1.5 million Cyberheist Ruins Escrow Firm

A $1.5 million cyberheist against a California escrow firm earlier this year has forced the company to close and lay off its entire staff. Meanwhile, the firm's remaining money is in the hands of a court-appointed state receiver who is preparing for a lawsuit against the victim's bank to recover the stolen funds.

More Online Banking Heists

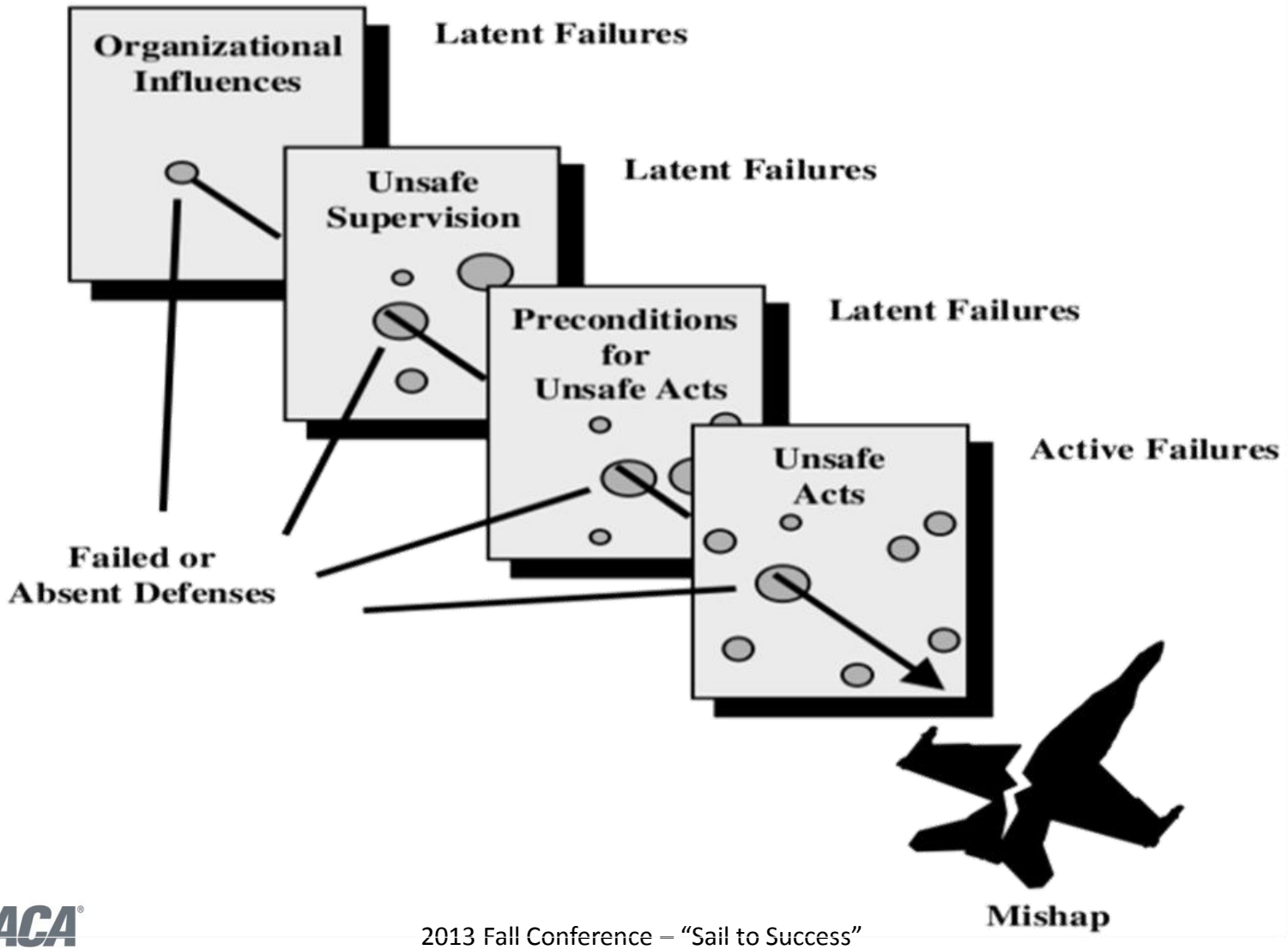
- Banks largely off the hook due to contract
- Money mule recruiting bottleneck
- Small biz victims list

3. The Swiss Cheese Effect and Patterns…Putting FUD in Context

The Swiss Cheese Effect and Cyber Security

- "Big" issues vs. small problems
- "Flying an airplane"
- Small compromises to full breach

The Swiss Cheese Effect



Small Problems Lead to Crash

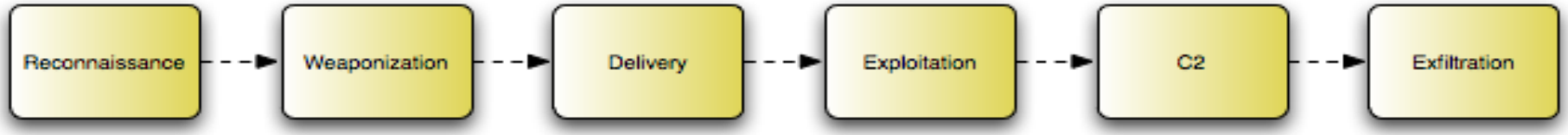
- Errors
  - Skills
  - Decisions
  - Perceptual
  - Comms
- Violations
  - Routine
  - Exceptional
- Bad Result
  - Plane Crash

Small Vulnerabilities

- Chain of events leading to catastrophe
- Mandiant report on S. Carolina Revenue Dept
- *Discussion*
- Bad Result:
  Data Breach, Governor at pressers

Small Vulnerabilities and the Kill Chain

- Cyber Kill Chain™



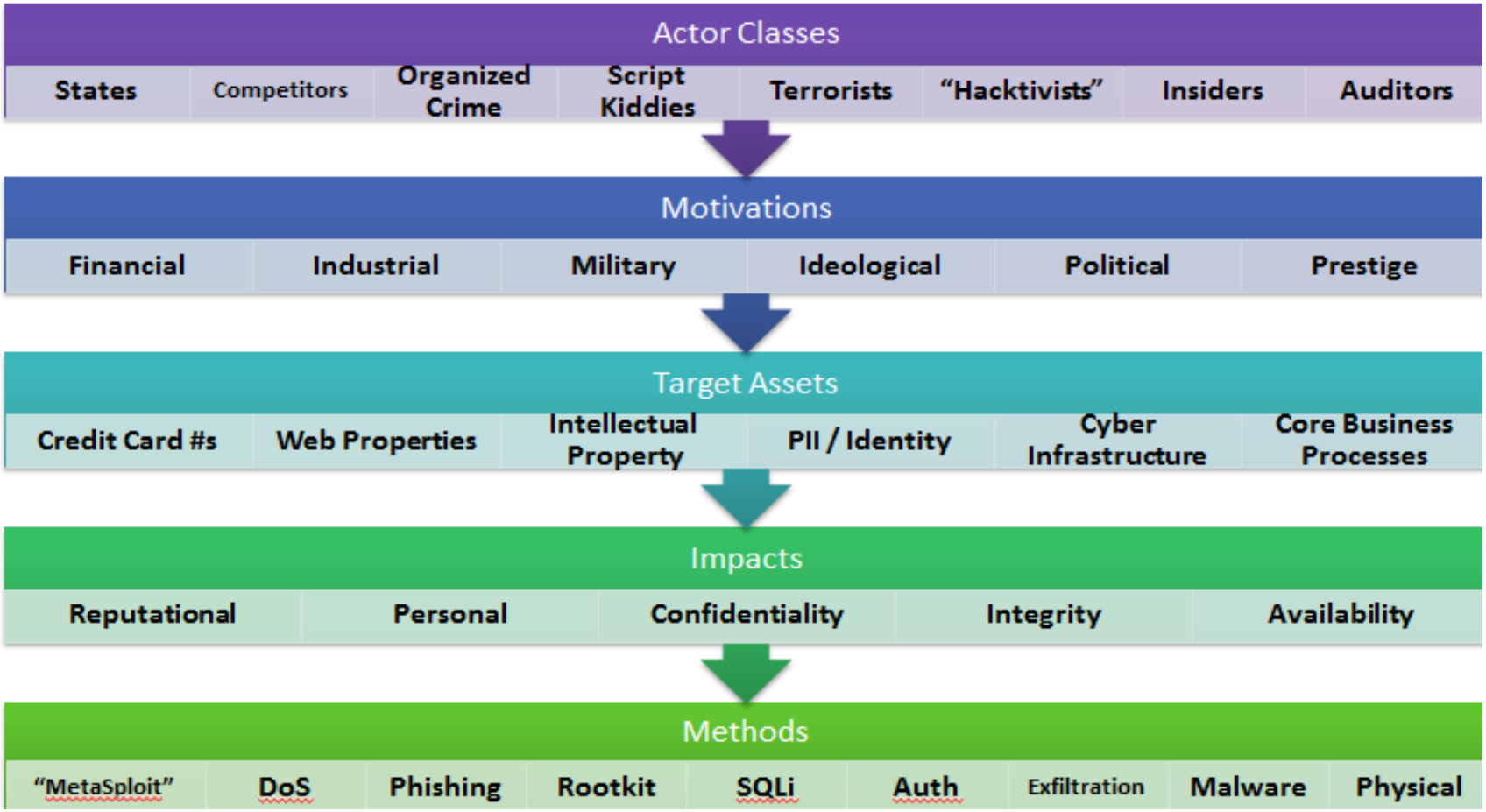
- Data Breach Triangle and/or the Cyber Kill Chain™
- Don’t stop every phase: delay, detect, contain…
- Attacker: Get in, get data, get out <-- Getting in is easy
- “Force Attacker Perfection” (Mogull)

Small Vulnerabilities, Patterns and Decision-Making

- Breach detection & Bejtlich's 5
- Majority of breaches discovered externally
- Verizon DBIR, a "how to" guide
- There are discernible attack patterns!
- Let's investigate using the Corman-Etue visuals…

Corman-Etue Attack Patterns

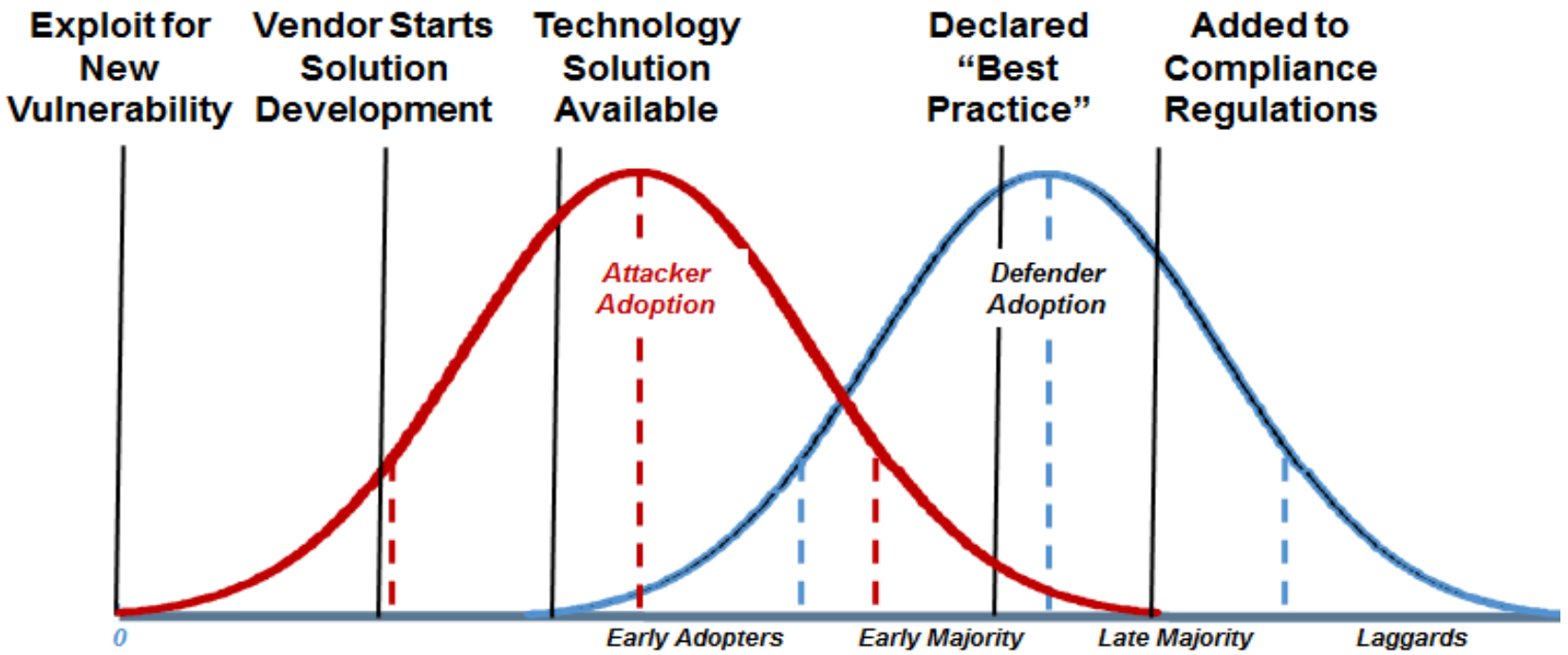
A Modern Pantheon of Adversary Classes



Cycle-time

(from Corman-Etue)

Solely Managing Vulnerabilities Will Never Win



Extensive Lag Between Attack Innovation, Solution, and Adoption

Organized Crime

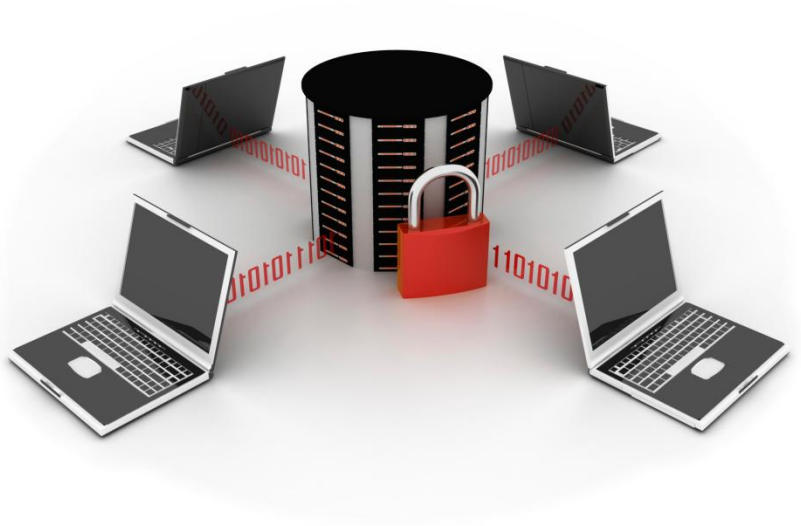
- Organized Crime
- Profit
- Fungible, Banking
- Confidentially
- Malware, Botnets, Rootkits

More Decision-Making Information

- Mandiant Breach Reports:
- Audit detection and notification response process
- Basic metrics in place?
- Why are we spending most of our money on AV?

Small Vulnerabilities and Some Focus Areas

- Patch 3rd party apps (flash, java,…)
- Test web apps (SQLi, XSS,…)
- Database security basics
- Time-to-detection of breaches



More Focus Areas

- Basic network segmentation (no desktop-to-desktop)
- Basic network segmentation (clinical vs. corporate)
- Move off XP & IE6… (by April of 2014)
- Basic ID & Access Mgmt: HR/Ops
- Understand “who & why and how”

4. Real or FUD (Fear, Uncertainty, Doubt)?

Common Corporate Issues
FUD or Not FUD

- Mobile & BYOD
- Moving to the Cloud
- Insider Threats / Contractors
- DDoS
- Application Layer Attacks
- Virtualization Security
- PRIVACY

Mobile: What Matters

- Pretty likely
  - Android app store
  - Android fragmentation
  - eDiscovery
  - Loss or theft
- Less likely
  - Malware on iOS

Mobile: Examples

- “Unlock screen” …then what?
- “Cached credentials”?
- Malware vs. theft
- Remote OTA (over the air) wipe limitations
- Malware: iOS vs. corporate XP
- Marketing message is… :-/
- Reality…

Cloud: What Matters

- Pretty likely
  - Visibility
  - Same old app-layer & db attacks
  - Logging helps
  - Auditability CSA Cloud audit mappings
  - Amount of control in SaaS/PaaS/IaaS
  - Location
- Less likely
  - Virtualization escape
  - Other side channel

Insider Threat: What Matters

- Real Issues
  - Accidental/Unwitting
  - Social engineering
  - Disgruntled admin.
  - Someone with IP access
  - Database security basics still apply
- FUD
  - Snowden
  - Wikileaks

Insider Threat: Accidental

- Unsanitized data in test environment
- Firewall rule changes
- Spearphishing email links/attachments
- Downloading the PII DB to unencrypted laptop

Time to surrender to the cloud?

Yes, in some limited way.

Know data sensitivity & consumption patterns

Insider Threat: Example

- Deliberate:
  "Of MICE and Men"
- Money, Ideology, Compromise, Ego
- Healthcare examples
- Finance examples

DDOS: What Matters

- Good ideas: Prepare
  - Internal infrastructure & public/internal separation
  - 3rd party services
  - Pre-existing ISP Ops, law enforcement contacts
  - What draws hacktivists
- Reality:
  - Low chance
  - Mitigate, you'll live
  - Unless you're a X-mas retailer :-/
  - DDoS as distraction?

Application Security: What Matters

- Real Issues
  - Supply chain
  - Home-grown code
  - Devs not trained

    and/or not rewarded for secure code
- FUD
  - DevOps inherently insecure
  - Can't test in production (Better late than never!)
  - Mobile malware?

Specialized Issues

- More discussion of types of threats
  - State sponsored
  - Organized attackers
  - Hacktivists
  - Lone hackers
  - They all want to be *effective, not 'sophisticated'*
  - Advanced is being good, not showing off 0dayz
- Specialized Industries:

  energy, healthcare, financial

5. “What Can an Auditor Do to Help Security?”

What Can IT Audit Do?

- Prioritize and allow innovation
- Understand what matters to you and attackers
- Check it's appropriately protected
  - Use appropriate security specialists to inform checklist update process

IT Audit: Responsibilities & Constraints

- Often do not have all the expertise
- Responsible for:
  - Checking security dept. work
  - Elevating issues
- How to recognize these issues?
- How to be more effective?

Technical IT Security:
Understanding Strengths & Limitations

- Priorities & Bonsai Trees
- If you have 10,000 desktops…?
- Classify people/endpoints/data
- Context for access helps with controls
- Is it IP because you say so?

Working Within the Corporation: Addressing Real Issues

- IT Security, IT Audit, Audit Committee
  - Together address Cyber Security Issues
  - Constantly changing environment
- Understand real threats to business
  - Then agree on importance
- Agree on determinants to elevate issues

Corporate Key Roles

- Audit Committee & Board of Directors responsible to raise the issue
- Executive Teams
- IT Security
  - Daily tasks vs. emergencies
  - Advanced threats
- IT Audit
  - With external specialists

Non-traditional Audit Focus

- Procurement bias:
  - Affecting HW/SW/MSSP/Consulting purchases?
- HR:
  - Not understanding the infosec community?
- Legal:
  - Aware how infosec works?

Key Focus Areas (Review)

- Patch 3rd party apps (flash, java,…)
- Test web apps (SQLi, XSS,…)
- Database security basics
- Time-to-detection of breaches
- Basic network segmentation (no desktop-to-desktop)
- Move off XP & IE6… (by April of 2014)
- Basic ID & Access Mgmt: HR/Ops
- Understand “who & why and how”

THANK YOU

@SHPANTZER

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Appendix

- Security Outliers (one hour video) http://vimeo.com/17854709 Swiss Cheese Effect
- Securosis “Force Attacker Perfection” https://securosis.com/blog/force-attacker-perfection
- Soft targets: business partners and law firmsht http://www.abajournal.com/news/article/banks_new_rules_lead_to_law_firm_cybersecurity_audits/
- Increased Regulation: Privacy: http://bits.blogs.nytimes.com/2013/01/10/california-suggests-mobile-app-privacy-guidelines/?_r=0
- Small vulnerabilities
  - http://governor.sc.gov/Documents/MANDIANT%20Public%20IR%20Report%20-%20Department%20of%20Revenue%20-%2011%2020%202012.pdf
  - http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain
  - https://securosis.com/blog/the-data-breach-triangle
- Notable ongoing failures http://www.va.gov/oig/publications/report-summary.asp?id=2760
- Online banking heists: Small victims list
  - http://krebsonsecurity.com/category/smallbizvictims/
  - http://www.speakoutsmallbusiness.com/view-post/The-Cost-of-a-Data-BreachCan-Bankrupt-Small-Business
  - http://www.ipost.com/blog/data-breaches/the-shocking-truth-about-smallbusiness-data-security-is-on-the-back-burner/
- Decision-making info: Verizon DBIR, a “how to” guide https://securosis.com/blog/how-to-use-the-2013-verizon-data-breach-investigations-report
- Mandiant Breach Reports: https://www.mandiant.com/resources/m-trends/#