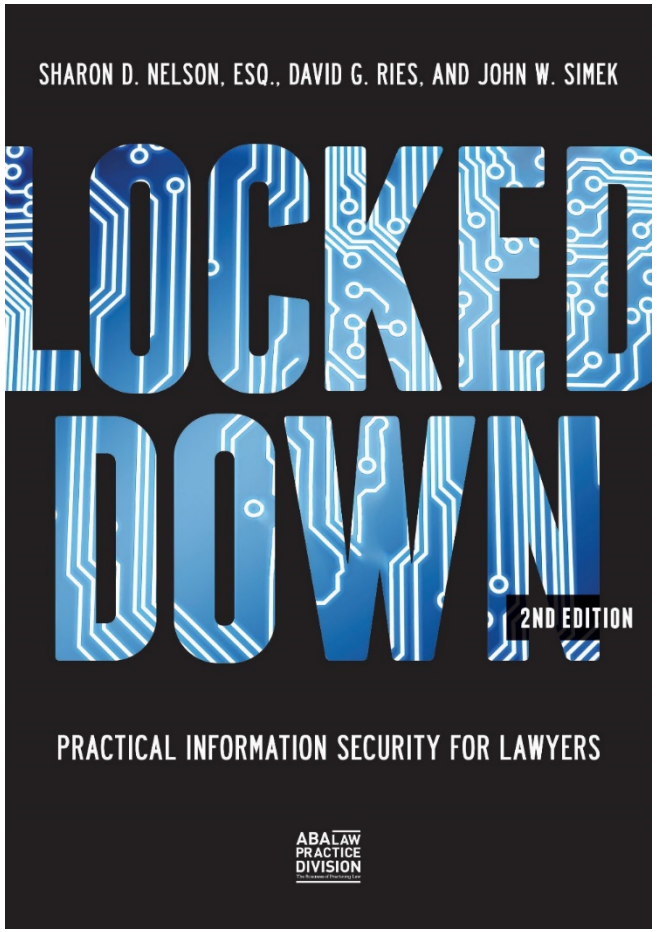
World War III: The War Against Data Breaches

Sharon Nelson and John Simek
President and Vice President, Sensei Enterprises
snelson@senseient.com; jsimek@senseient.com
www.senseient.com 703.359.0700
@sharonnelsonesq

JOLT - February 24, 2017
U of Richmond Law School


SHARON D. NELSON, ESQ., DAVID G. RIES, AND JOHN W. SIMEK
LOCKED DOWN
2ND EDITION
PRACTICAL INFORMATION SECURITY FOR LAWYERS
ABA LAW PRACTICE DIVISION


ENCRYPTION MADE SIMPLE FOR LAWYERS
DAVID G. RIES / SHARON D. NELSON / JOHN W. SIMEK

Worried about a data breach? You should be.

Breaches from the Am Law 200

- March 29 – *Wall Street Journal*
- Cravath Swaine and Weil Gotshall
- Breached in summer of 2015
- Other firms also breached
- Source? Unknown but CS confirmed "limited breach"
- Not aware of any improper use of info

Weil

CRAVATH, SWAINE & MOORE LLP

Russian cybercriminal looking for hacker assistance

- March 29, *Crain's Chicago Business*
- *"Oleras"* posted in cybercriminal forum
- Offered more than $100,000 plus 50-50 of profits exceeding $1 million
- Insider info sought for stock market gain
- Almost 50 firms listed as targets
- A "Who's Who" of law firms
- Two already breached – Cravath and Weil

Data breach class action planned against elite law firms

- March 31st, *Law360*
- Edelson PC
- Investigated for more than a year
- Law firms (not yet named) not complying with data breach laws
- 5/6 The Global Legal Post: Filed one privacy class action against a Chicago law firm (under seal) but now seeking to unseal since breach is resolved
- State attorneys general expected to investigate – maybe FTC

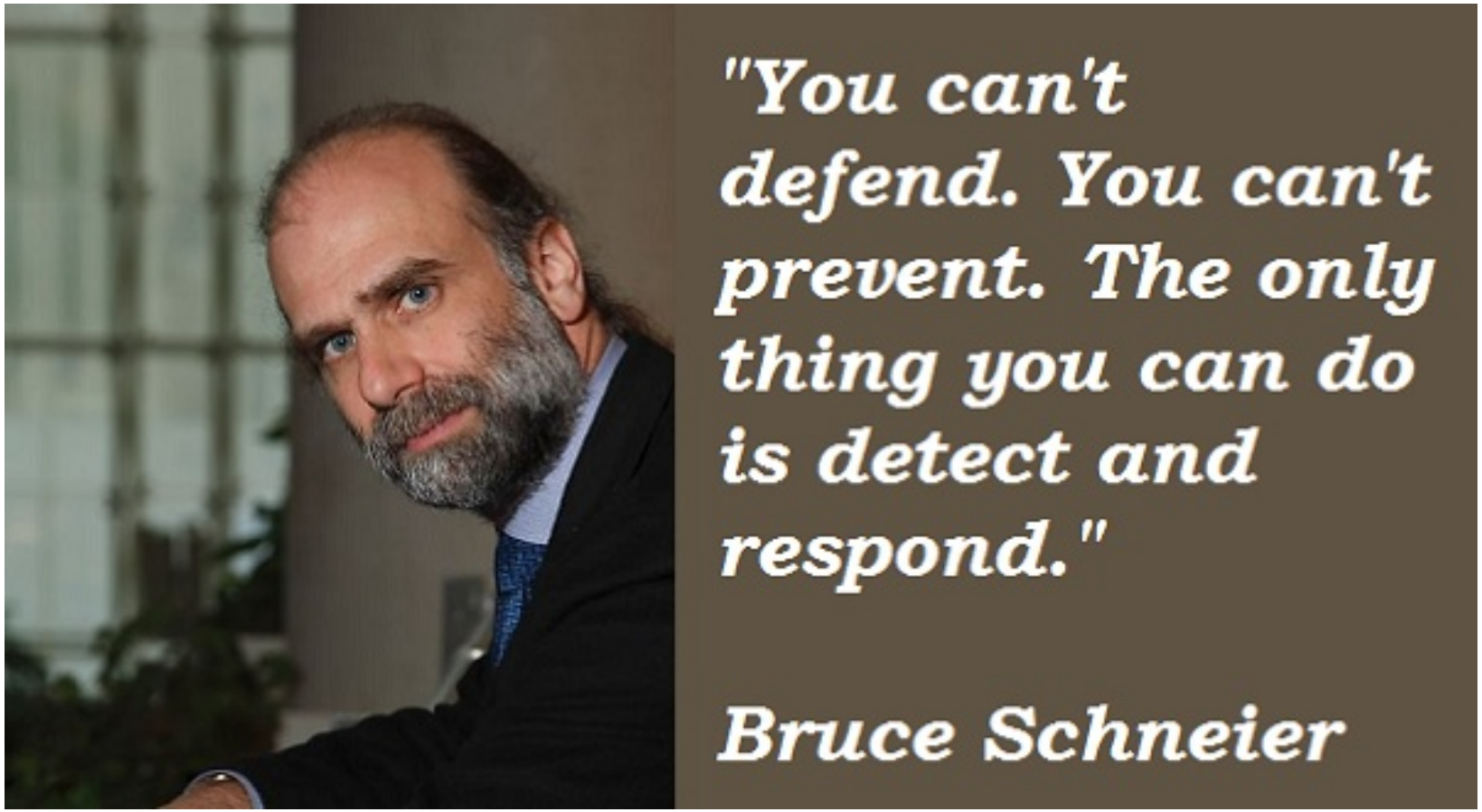
December 2016

- Edelson PC filed class action suit in April (unsealed in December) against Chicago's Johnson & Bell alleging that lax security put client data at risk
- No harm alleged
- When notified, firm fixed all vulnerabilities
- Unjust enrichment theory – fees presumed to include industry standard security of data
- Has moved to confidential arbitration

World's largest data breach? A law firm

- April 5, *The Guardian: "The Panama Papers"*
- Mossack Fonseca, 11.5 million files
- 1977-present, 2.6 terabytes
- BBC – firm helped clients
  - Launder money
  - Dodge sanctions
  - Evade taxes
- Vladamir Putin – $2 billion
- Iceland PM Gunnlaugsson resigned. Once owned – and his wife still owns – an offshore investment company with multimillion-pound claims on Iceland's failed banks
- Security was trivial

Advanced hackers with advanced tools



Insiders: Reported 4/18/16

- Former IT engineer for Dallas law firm Locke Lord
- 9 Years Prison, $1.7 Million Fine
- Issued commands that caused "significant damage“
- "including deleting or disabling hundreds of user accounts, desktop and laptop accounts, and user e-mail accounts."

Locke Lord LLP

National Law Journal – May 2

- Law Firm Breaches Happening at Dizzying Speeds

May 9 – Second round of Panama Papers released

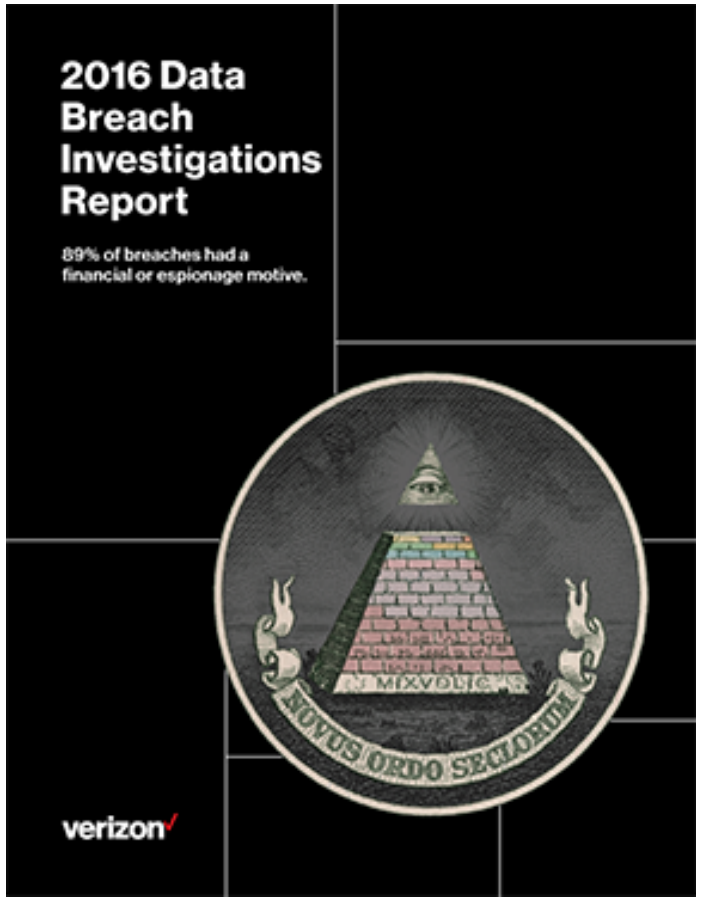
- Searchable by name/country
- International Consortium of Investigative Journalists
- More than 200,000 entities
- Akin Gump, Arnold & Porter, Baker & McKenzie, Bryan Cave, Dentons, DLA Piper, Greenberg Traurig, Hogan Lovells, Jones Day, K&L Gates, Linklaters, Morgan Lewis, Norton Rose, Orrick, Perkins Coie, Square Patton Boggs, Squire, Sanders & Dempsey, Troutman Sanders, White & Case, Wilmer Cutler – and the list goes on

2016 Verizon data breach report

- Covers over 100,000 incidents, of which 3,141 were confirmed data breaches – 82 countries and many industries
- 89% of breaches had a financial or espionage motive
- 63% of data breaches involved weak, default or stolen passwords
- 30% of breaches due to human error
- 93% of breaches occurred with minutes, 11% within seconds
- Less than 25% discovered in a few days
- Bad guys have a big head start!

"I suppose I'll be the one
to mention the elephant in the room."

2016 Verizon data breach report



- 30% of users opened phishing e-mails
- 12% clicked on attachment with malware or link in e-mail
- 60% of breaches happened because of phishing e-mails
- Almost as many attacks on user devices as on servers
- 80% of attacks were external

December 2016

- Manhattan U.S. Attorney unsealed indictment against 3 Chinese men who used law firm employee credentials to access huge number of internal e-mails at Cravath Swaine and Weil Gotshal in 2015
- 2 firms represent 44 of the Fortune 100 companies in US
- Made more than $4 million in illegal stock trades
- Spear phishing attacks
- Attempted to hack into 7 firms
- Odds of success appears to be 2 in 7

December 2016 – some good news

- Security ratings report by BitSight – best protected industries
  - Financial
  - Legal
  - Retail
  - Healthcare
  - Energy/utilities
  - Government
- 1269 legal entities analyzed
- Not many solo/small firms
- A good number scored miserably
- Large firms scored the best

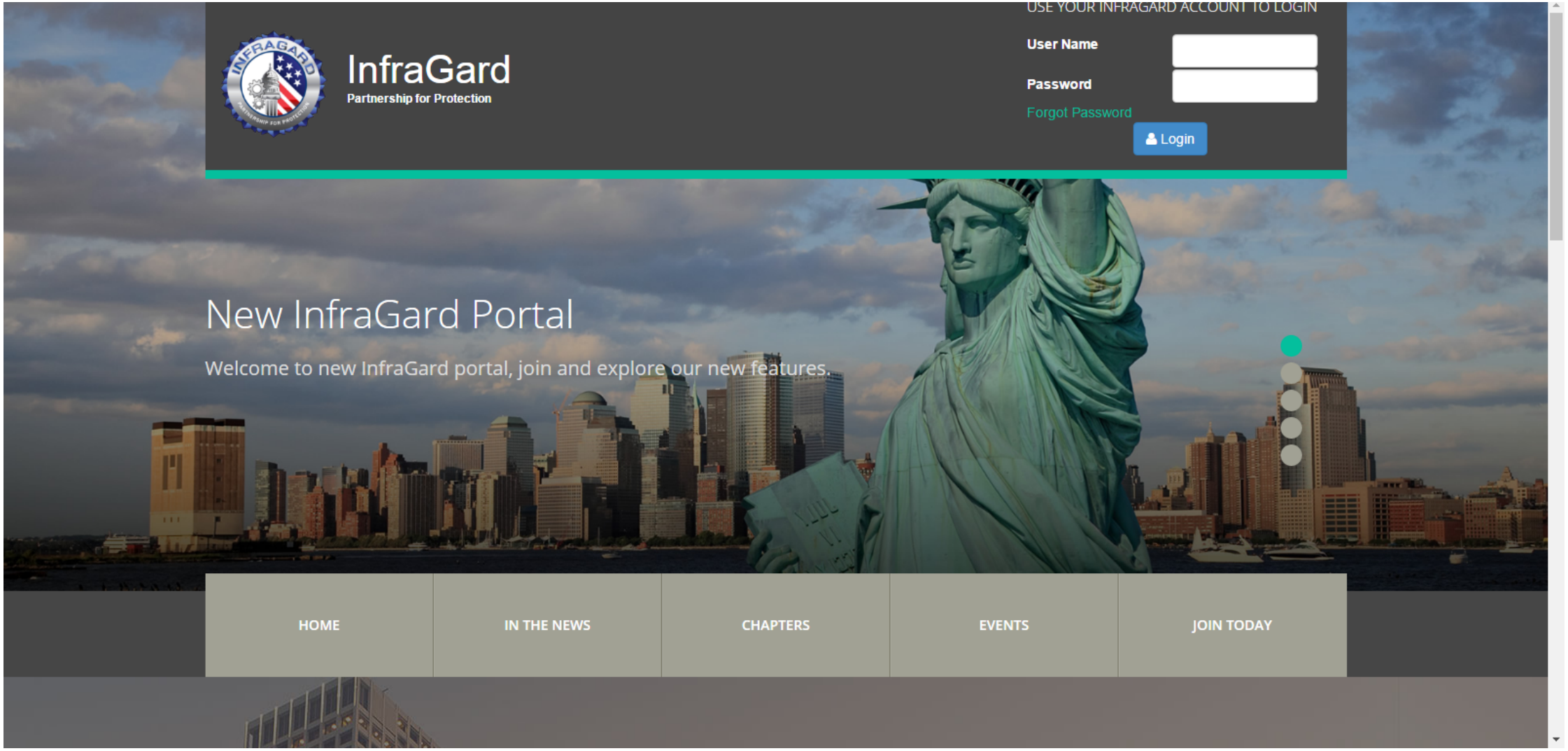
January 2017

- Ferguson, Praet & Sherman
- Researcher found accessible law firm files on the Internet
- Volume was astonishing
- Video surveillance appeared to show that two jail employees may have walked past inmate hanging himself, evidence not produced in investigation of the death
- Firm was synchronizing backup across the Internet without a password

Threat Actors

- Cybercriminals
- Hackers
- Hactivists
- Government surveillance
- State sponsored / condoned espionage
- Insiders (disgruntled / dishonest / bored / untrained)

InfraGard


USE YOUR INFRAGARD ACCOUNT TO LOGIN
InfraGard
Partnership for Protection
User Name
Password
Forgot Password
Login
New InfraGard Portal
Welcome to new InfraGard portal, join and explore our new features.
HOME
IN THE NEWS
CHAPTERS
EVENTS
JOIN TODAY

Law firms spending record amounts on cybersecurity

- Chase Cost Management Survey Large law firms spending average of 1.9% of gross annual revenues
- AM LAW 200 – as much as $7 million per year

Practical Security Steps

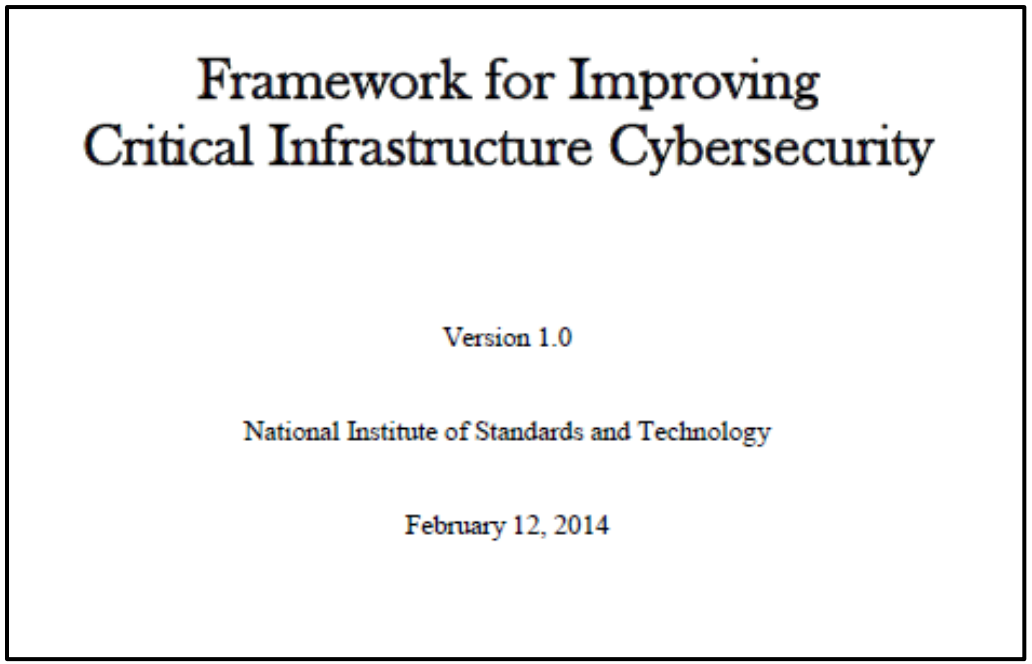
We can’t keep the barbarians at the gates

- Identify and protect – old mantra
- Now, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER

Biometrics and 2FA

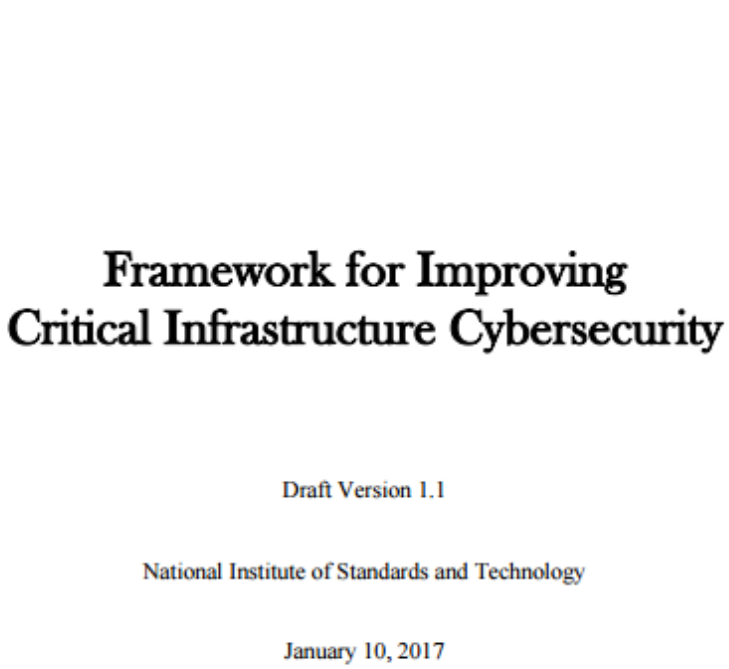
- Biometrics is not a good solution – once your biometrics are owned, they will always be owned (voiceprints, fingerprints, retinas) – 5.6 million fingerprints stolen in OPM breach
- 2FA is here and growing rapidly – enable wherever you can
- Best protection? Something you know, something you have and something you are

NIST Cybersecurity Framework: Small Business Information Security: The Fundamentals (30 pages)



DRAFT NISTIR 7621 Revision 1
Small Business Information Security: The Fundamentals
December 2014 – up to 500 employees
ISO 27001

Draft revision issued January 10, 2017


Framework for Improving
Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017

- Details on managing cyber supply chain risks
- Clarifies key terms
- Introduces measurement methods for cybersecurity
- Remains consistent with 2014 document
- Comments due April 10

First Five Quick Wins – Center for Internet Security

Part of the *CIS Controls for Effective Cyber Defense Version 6.0*

1. Application whitelisting
2. Using common, secure configurations
3. Patch application software within 48 hours
4. Patch systems software within 48 hours
5. Reduce the number of users with administrative privileges.

- Would have prevented 85% of security incidents (Australian Signals Directorate)

Enterprise security software

- Anti-Malware
- Anti-Spyware
- Internet Suites
  - Trend Micro
  - Webroot
- No silver bullet
- Some will come into your network

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS
  - Monitor inbound and outbound activity
  - Passive monitoring
  - Suspicious activity
  - Triggered actions
- IPS
  - Monitor network activity
  - Active monitoring
  - Attack behaviors
  - Automated action
  - Host-based
  - Network-based

Cisco Meraki – from several hundred dollars a year, Palo Alto Networks for larger firms

The most common failings

- Not applying security patches or other critical updates
- Relying on outdated software for budgetary reasons – or from sheer fear of upgrading and having to learn new software!
- Microsoft XP, Server 2003, Office 2003, IE 10 and earlier
- Apple QuickTime for Windows
- Office 2007 support ends October 2017
- Exchange 2007 support ends April 2017

iOS 10 & macOS Sierra

- iPad 1, 2, 3
- iPad Mini
- iPod Touch 5th Generation and Older
- iPhone 4S and older
- MacBook (early 2009 and older)
- iMac (early 2009 and older)
- MacBook Air (2009 and older)
- MacBook Pro (2009 and older)
- Mac Mini (2009 and older)
- Mac Pro (2009 and older)

News from Microsoft January 2017

- Microsoft 7 is so outdated that patches can't keep it secure. Extended support ends 1/13/20. No longer receives patches unless you have a pricy Microsoft Custom Support Agreement
- Microsoft 10 security: "So good, it can block zero-days without being patched."
- Overstated, but a darn good operating system with new tools to defeat exploits

Training Training Training
Have We Mentioned Training?

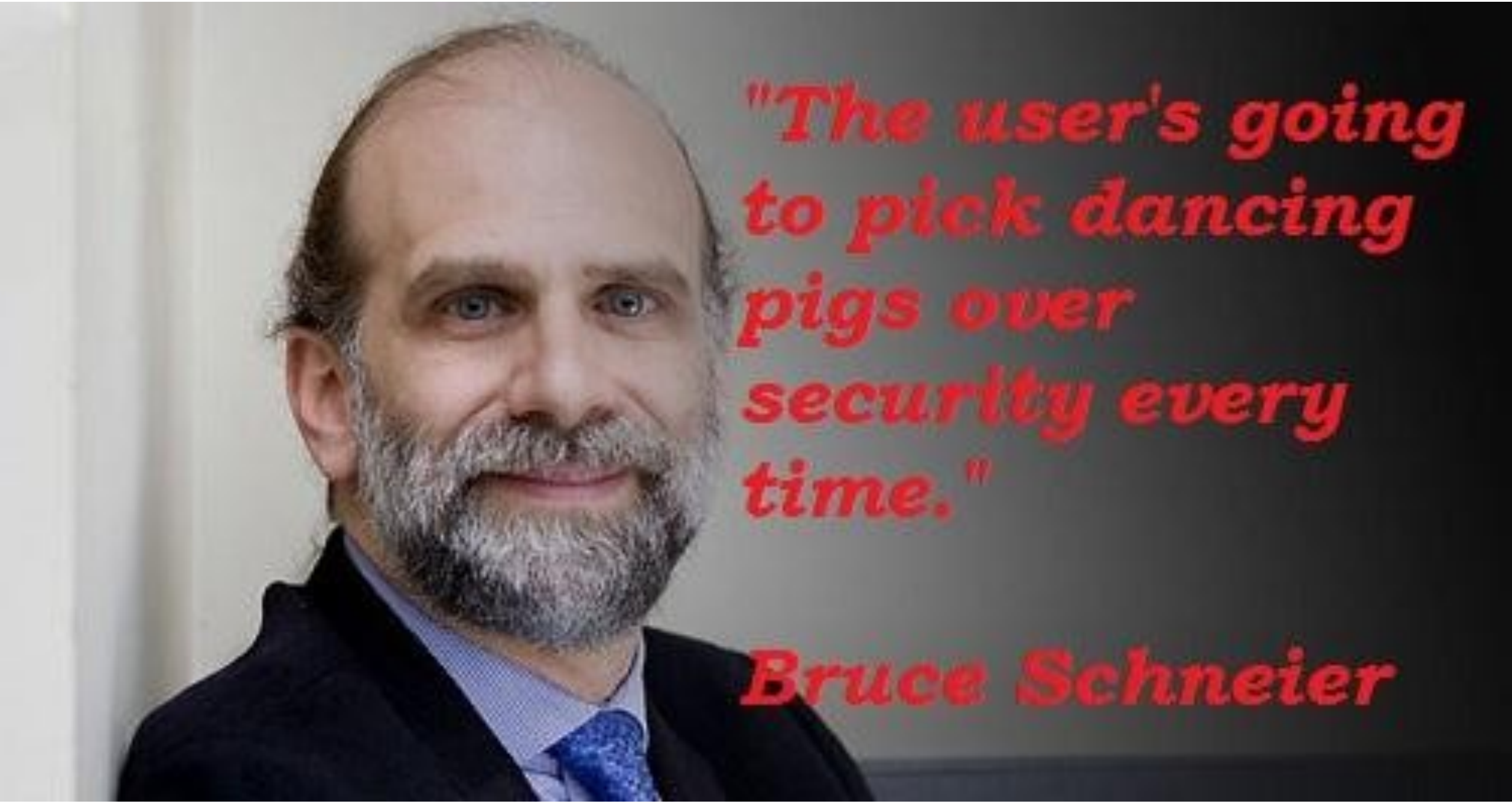

Allways chek for
speling erors

91% of hacking attacks begin with a phishing e-mail

- 2016 PhishMe study
- Why do users click?
  - Curiosity (racy New Year's photos)
  - Fear (bar complaint attached)
  - Urgency (boss needs this today)
  - Recognition (award you've gotten)
- SonicWall and OpenDNS
- One phishing simulation (reported to employees) drops risk of phishing success by 20%

Training

- Phishing, especially spear phishing – most successful way of breaching law firms – an e-mail from a friend/colleague can be spoofed. Hackers research personal details too – may know nickname
- CEO scams – FBI alert, 2.3 billion, 270% increase Jan. 2015-Feb. 2016
- Drive-by infections
- Sharing credentials
- Baiting (flash drives)
- Piggybacking
- Hitchhiking
- Social engineering
- Train annually!


"The user's going to pick dancing pigs over security every time."
Bruce Schneier