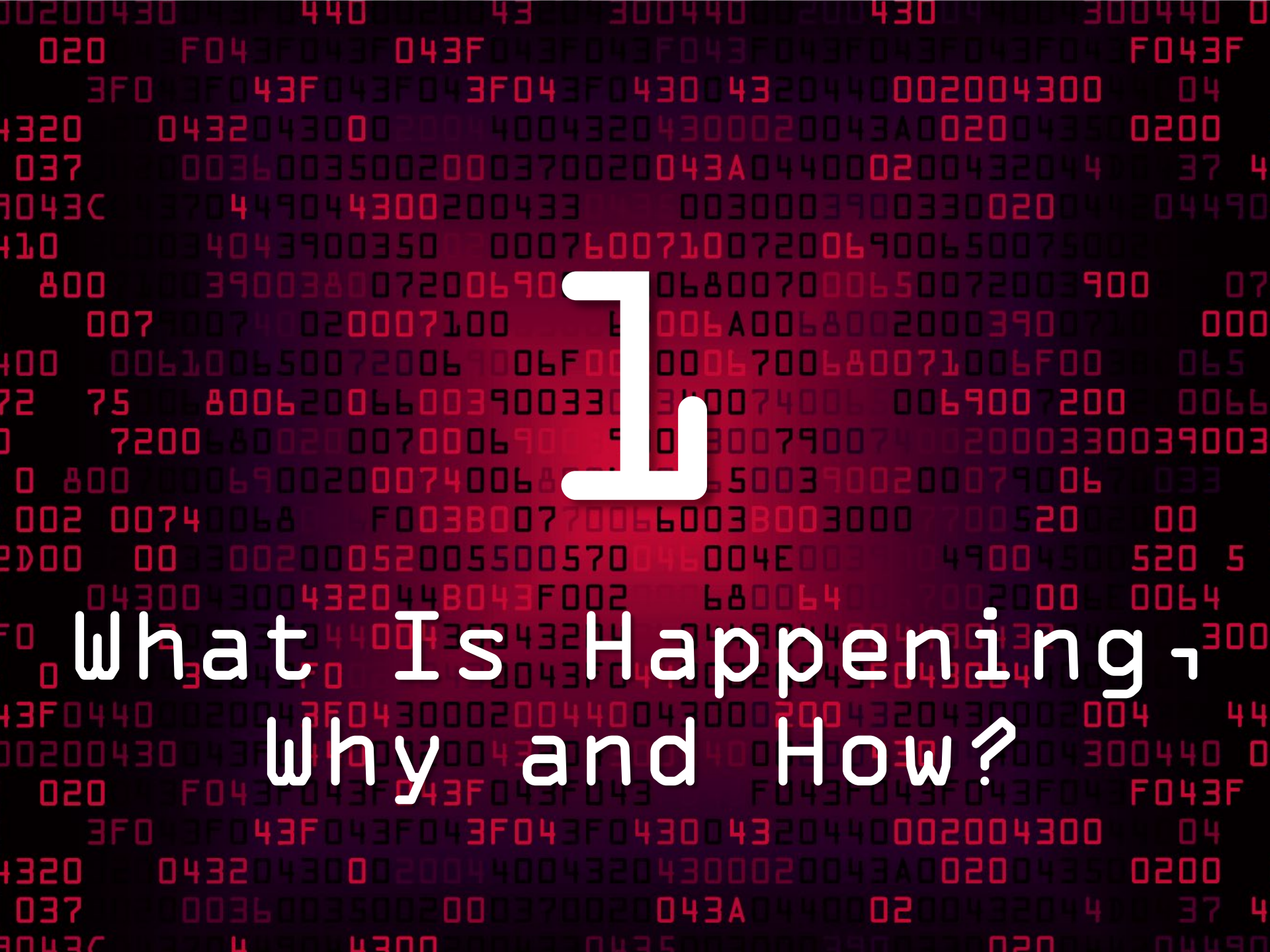
CYBERSECURITY

Making Sense of It All

J. Stephen Britt, Esq.
Cybersecurity Practice Manager

BERENZWEIG LEONARD

Table of Contents


What Is Happening,
Why and How?

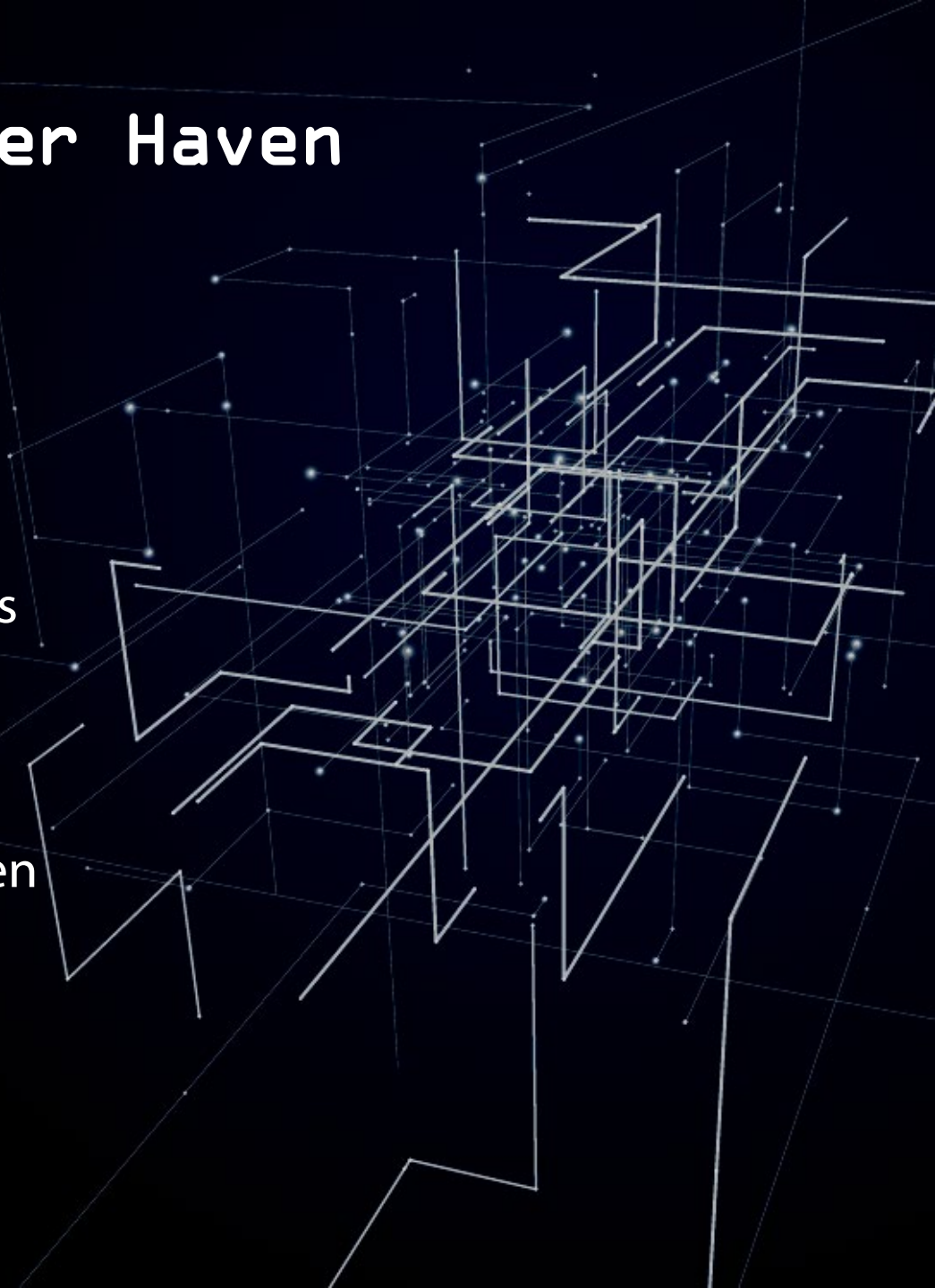
Who Commits These Crimes?

- Financial Criminals
- Caused-Based Hacktivists
- Corporate Espionage
- Blackmail
- Competitive Advantage
- Nation-States
- Organized Cyber Criminals


Power
Low Risk
Why do they do it?
Money
Cheap
Easy

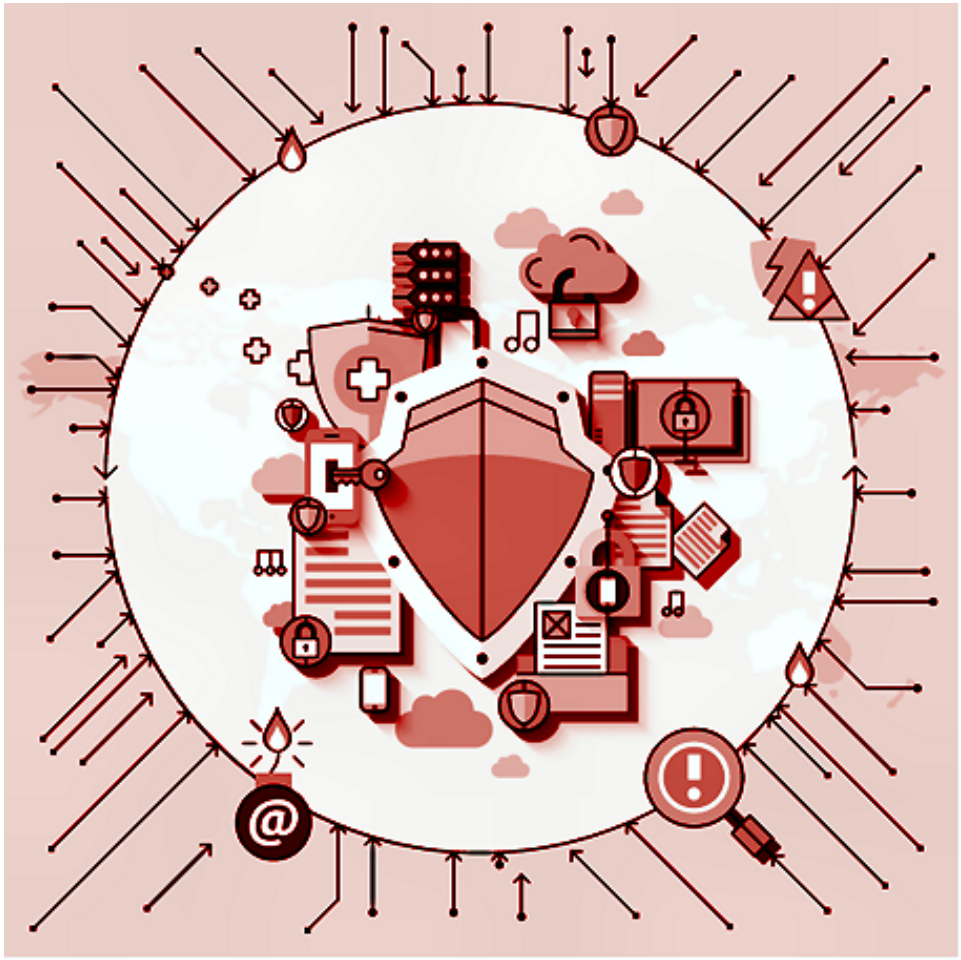
Dark Web: Hacker Haven

- Network of servers support anonymous communication
- Special software provides access to these hidden sites
- The Dark Web posts stolen PII and hacking/malware tools



The Security Model Is Broken

- "Keep 'Em Out"
- Firewalls & anti-virus only
- Treats all assets and data the same
- Assumes the network perimeter is static
- Assumes employees can be trusted and everyone else cannot



What Has Changed?

- IT is mobile – BYOD (phones, laptops, watches, etc.)
- Server virtualization, application servers
- Legacy security tools do not interoperate

The New Network Security Model

You can't protect against what you can't see – too much network traffic is missed or invisible

The Risk Landscape

- Unintended disclosures
  - Paper records
  - Electronic assets
- Lost, missing, stolen devices
- Human error
- Rogue employees
- Phishing attacks
- Intrusions, hacks, malware, viruses
- Ransomware

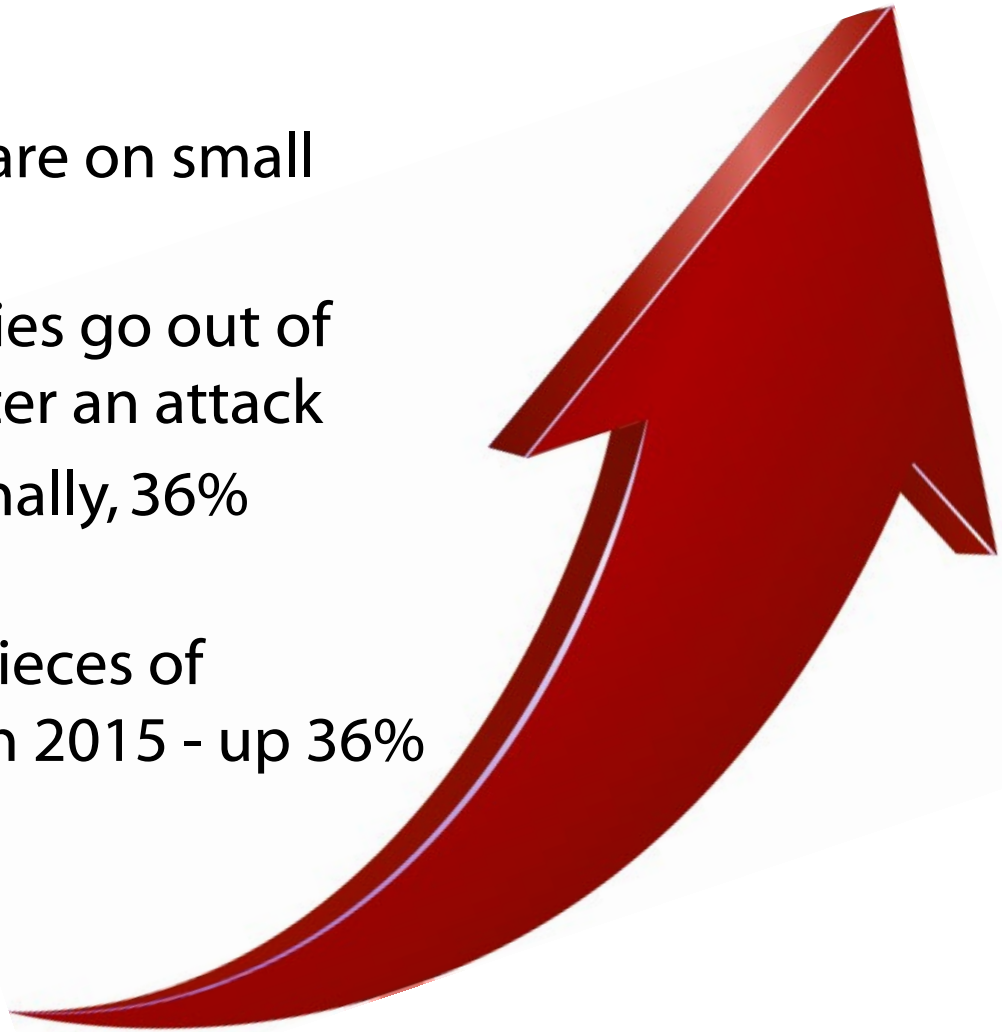
How Do They Do It? Common Attack Vectors

- Scans for unprotected or unpatched systems
- Scans for remote or retired servers left online
- Attacks on inactive user accounts (temps and contractors)
- Password guessing, cracking or privilege escalation exploits
- Social engineering scams, phishing and vishing
- Unpatched web sites or weak applications

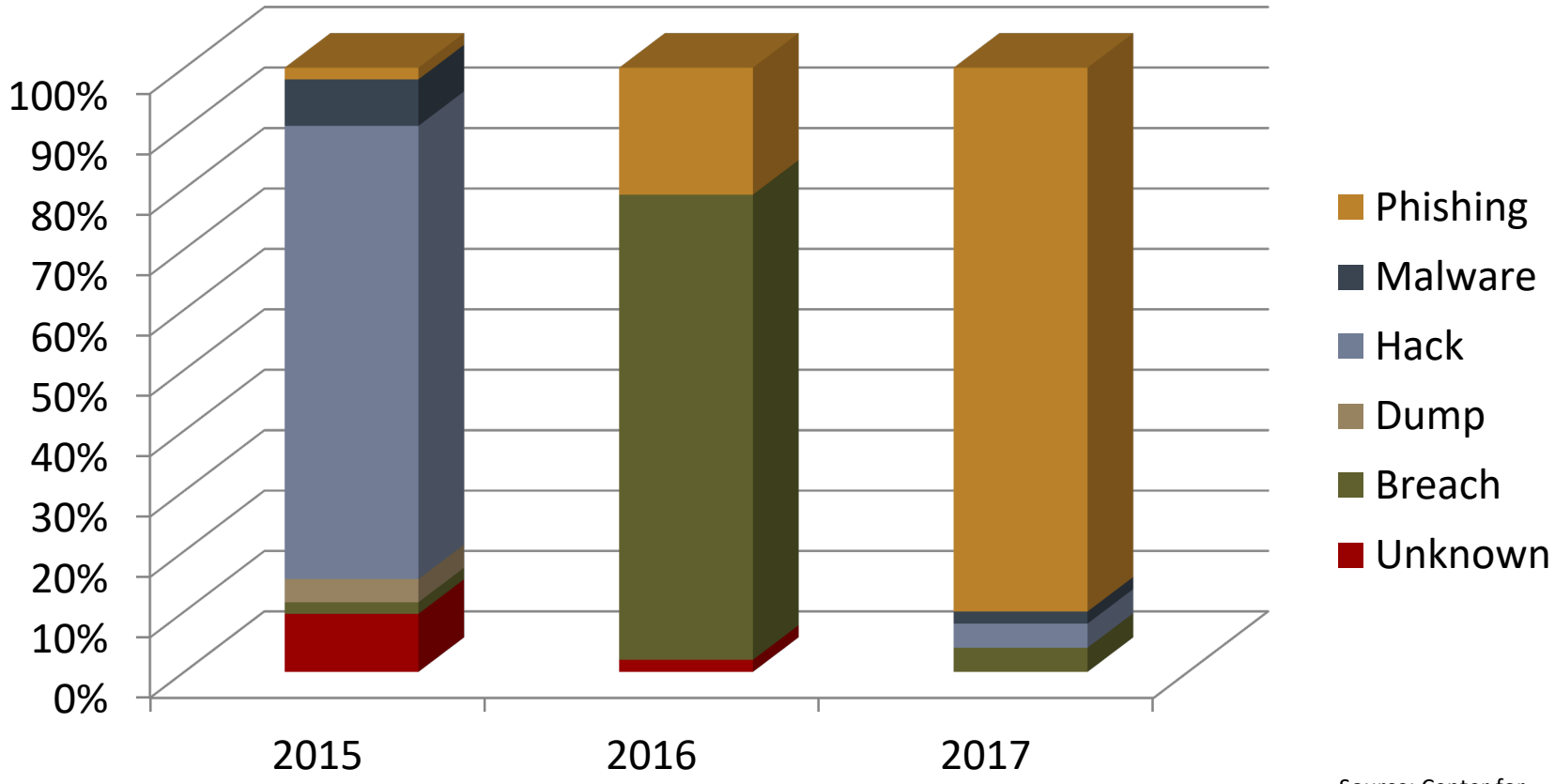

2
Attacks by
the Numbers

Attacks Are Growing Exponentially

- 43% of cyber attacks are on small business
- 60% of small companies go out of business 6 months after an attack
- 64% discovered internally, 36% externally
- 430,000,000 unique pieces of malware discovered in 2015 - up 36%

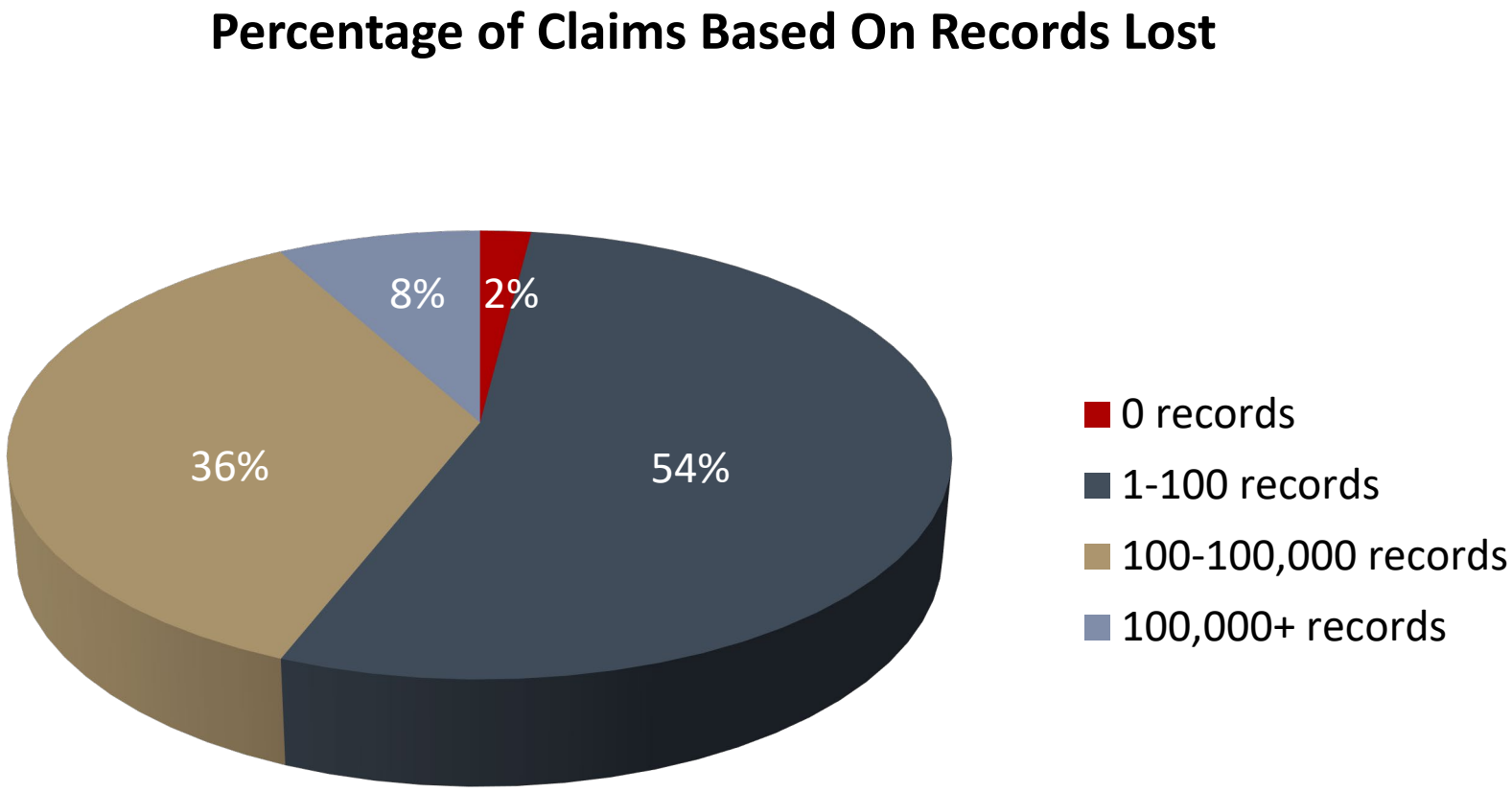


Sources of Reported Data Breaches

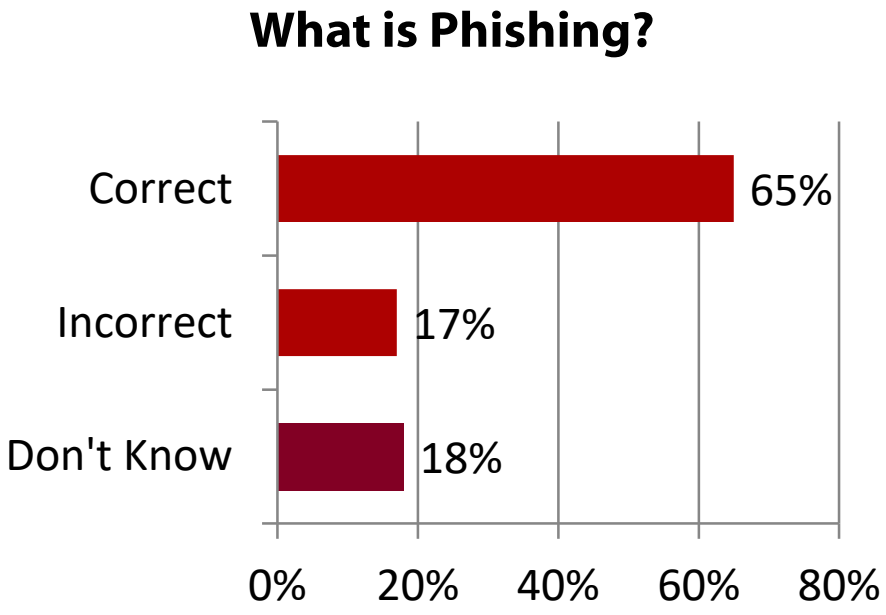


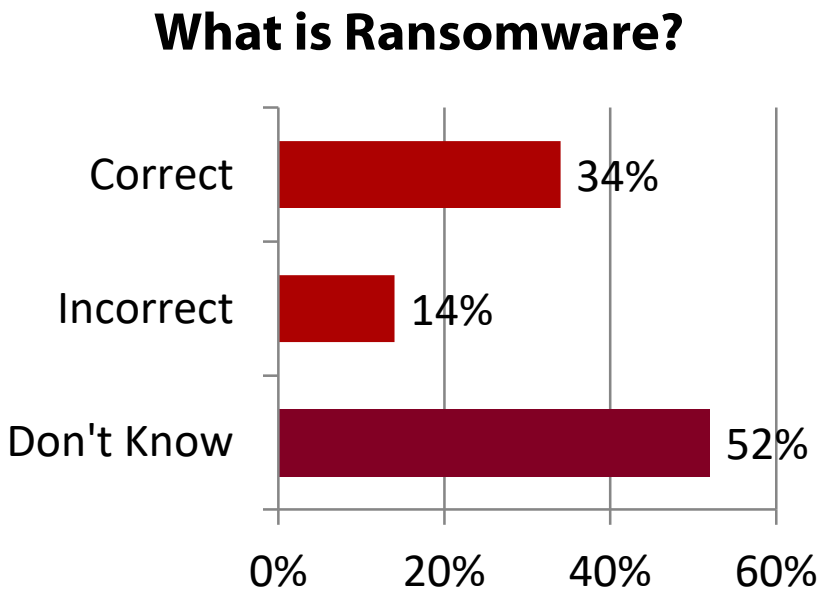
Source: Center for Internet Security

Too Small to Target?



The Wombat Security Survey





What Is Phishing?

The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers

What Is Ransomware?

A type of malicious software designed to block access to a computer system until a sum of money is paid

Don't Become a Ransomware Victim

LINKS

Avoid unknown links, ads, and websites

ATTACHMENTS

Don't download unverified attachments or apps

SOFTWARE

Keep software up to date and patch known vulnerabilities

BACKUPS

Backup data and files to a secure location daily or even hourly

The Internet of Things (IOT)

- 6.4 billion connected devices with 20.8 billion expected by 2020
- Devices with no data security:
  - Cars
  - Smart home devices like locks, thermostats, refrigerators
  - Medical devices
  - Smart TVs
  - Routers, webcams, internet phones
  - Google Home, Amazon Echo, Mattel Aristotle
- FitBit, Jawbone

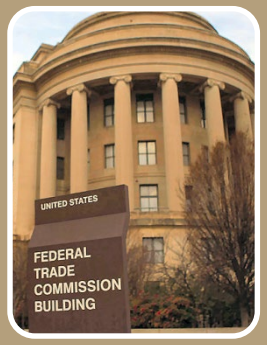
Social Engineering

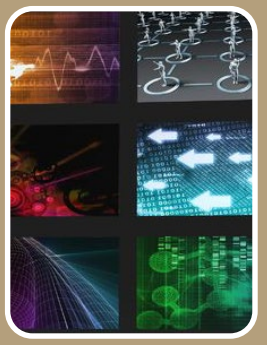
- Research and reconnaissance
- Review of social media profiles
- Learn victim's job, coworkers, and organizational structure
- Read online employee resumes

3

Legal Landscape

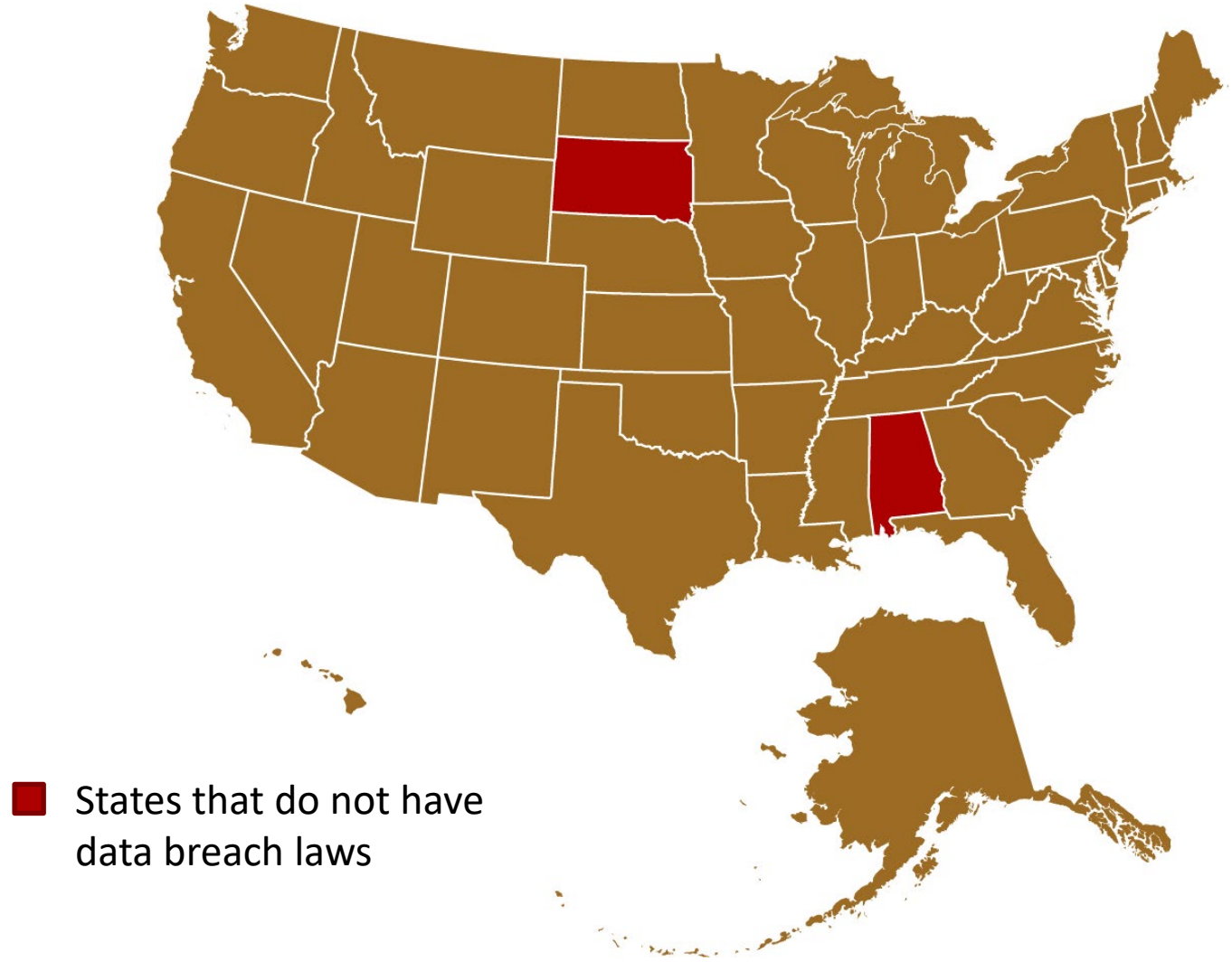
No Federal Data Breach Law





HIPPA	FTC	SEC	FCC	DoD DHS GSA	Payment Card Industry

State Data Breach Statutes – Personally Identifiable Info



Key Government Contractor Rules

- FARS Basic Safeguarding Clause (52.204-21)
- DFARS Network Penetration and Cyber Incident Reporting (252.201-7012)
- NARA Controlled Unclassified Information (CUI) (32 CFR 2002)
- FAR Privacy Act Training
- DHS Proposed Rule – Safeguarding DHS CUI (82 Fed. Reg. 6429)

Regulator Hot Buttons

- Lack of effort – not taking the risk seriously
- Unencrypted backup and mobile devices
- Default configurations and passwords
- Lack of policies
- Insufficient employee training
- Poor cyber hygiene
- Slow detection, notification and remediation
- Failure to follow own data privacy policies

Your First Call: The Lawyers

- Attorney-client privilege
- Attorney Work Product Doctrine

4 Real Life Stories

Shadow IT

DHS CDM (Continuous Diagnostics & Monitoring)

Small CPA Firm

- Small accounting firm
- Scan showed 25,000 credi cards
- Firm doesn’t take credit cards

Spear Phishing

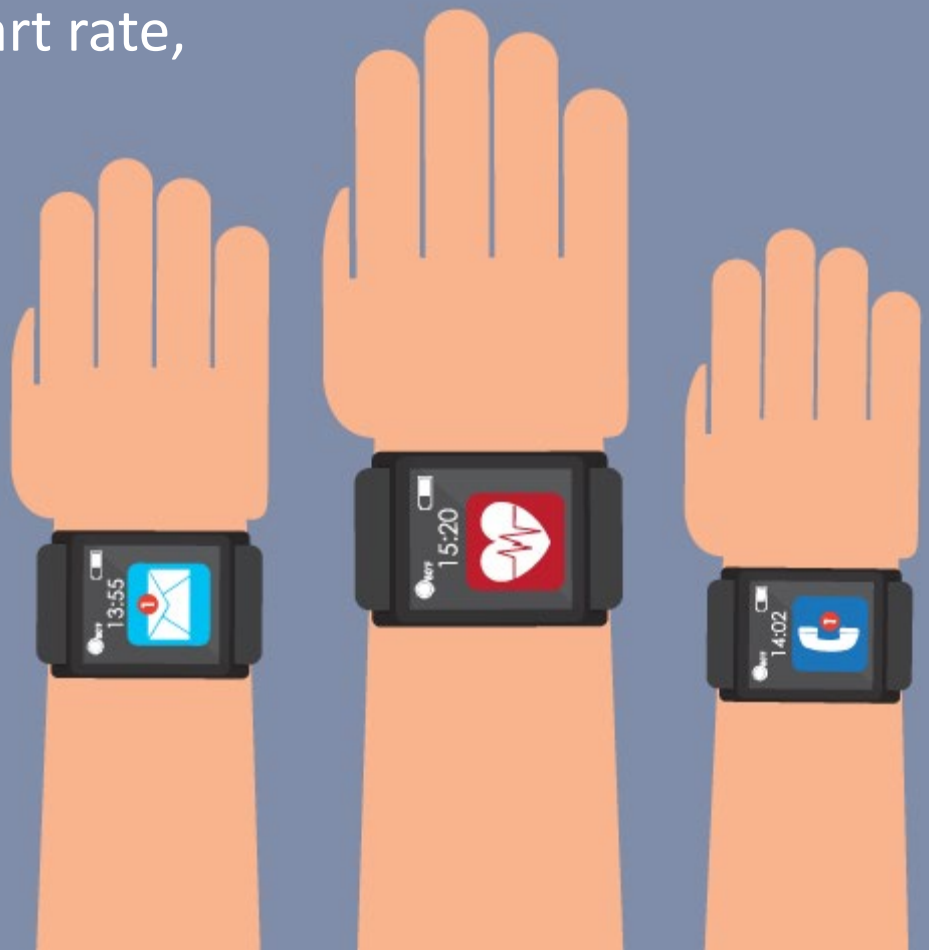
- Local GovCon - CEO email request
- Employees covered 38 states
- CISO and several employees quit

John Podesta

- In March 2016, receives fake Google email hack
- IT director says it was “legitimate,” meant “illegitimate”
- Said “change your PW immediately” but didn’t tell how
- 10 years’ worth of emails released

Wearables in Workplace

- 125 million units by 2019 (up 35%)
- Employers using wearables in corporate wellness programs
- Tracking employees' heart rate, blood pressure, etc.
- Data held by employers insecurely
- 14 states define PII to cover this data
- Programs can trigger HIPAA




5
Cyber Action Items

HR Roles and Responsibilities

- Employees are the weakest link in any security program
- Do not assume others understand
- Develop and implement employee training
- Ensure employee compliance
- Prohibit *unverified* W-2 / PII data transfer
- Get a legal review of outsourced HR/payroll data protection

Cyber Risk Management Program

Inventory assets
Know what is connected and what software is running

Prioritize assets
Segregate high-value data

Establish security & access controls & IR plan

Governance
Board, C-suite, IT, communications, contracts, HR, and legal

Employee policies and procedures

Continuously monitor, backup, scan, and audit

Employee Policies and Procedures

- Use of employer-owned equipment (BYOD)
- Company right to install controls on employee devices
- Use of storage media on company network
- Employer monitoring of electronic communications
- Personal activity on company time
- Password management policy
- Social media and blogging
- Harassment, bullying, discrimination, etc.
- Video recording policy (phones, cameras, etc.)
- Physical access & removal of company equipment
- Remote log-in rules
- Storage & return of data

Password Management - Time for Hacker to Bust Password

Character Length	Lowercase only	Lower + Uppercase	Lower, Upper, Numbers & Symbols
6	10 minutes	10 hours	18 days
8	4 days	3 years	463 years

- The four most common passwords
  - 123456
  - 12345678
  - qwerty
  - abc123

The Role of Cyber-Insurance

- Risk mitigation but only 19% of companies have it
- 1st Party v. 3rd Party (homeowners v 3rd party claims)
- Cyber coverages can be found in:
  - Crime Policy (only by rider)
  - D&O
  - Professional Liability (Technology E&O)
- But must understand exclusions/ sub-limits

Insurance Coverage Issues

- Cover cost of investigation & notifications – not remediation
- Costs not reimbursed until carrier notified
- Independent contractors may need own policy
- **Exclusions:**
  - Act of War and Terrorism – nation-state hack?
  - Best Practices – can exclude inadequate security
  - Voluntary Parting – CRIME policy
  - Fines & Penalties
- Social engineering needs endorsement
- May require victims to authenticate phish (call back)


6
Key
Recommendations

Big Picture Recommendations

- Don’t ignore the risk or threat – partial action is better than none
- Don’t let the perfect be the enemy of the good
- Don’t be the poster child – regulators should recognize good-faith effort
- Take a leadership role in your company.

Top 10 Take-Aways

1. Prioritize spending. Don't need to it do all at once.
2. Don't think "check the box" or "compliance" – think security.
3. Understand your business - how you hold sensitive data and how it is protected.
4. Team effort for every employee - not just IT or C-Suite.
5. Assess your network, learn vulnerabilities, remediate & monitor.
6. Prepare, train and enforce employee policies.
7. Ransomware is a game changer. Do frequent back-ups.
8. Security is not "one and done" or "one size fits all."
9. All government contractors - get NIST 800-171 certified now.
10. Create an IR Plan. Engage legal counsel and a breach assessment firm now.

A Good First Step

BERENZWEIG LEONARD

For: BBG Seminar Attendees

Task: **Baseline Cyber Security Risk Assessment**

- Attorney-client -protected engagement
- 1-hour onsite interviews (25 questions)
- Nessus network scan of up to 500 IP addresses
- Hemisphere technical action report
- Legal review of scan report and operations
- Berenzweig Leonard action report

Cost: Fixed fee of $5000


Q
A

Contact

J. Stephen Britt, Esq.

Berenzweig Leonard LLP

Director, Data Security & Privacy

8300 Greensboro Drive, Suite 1250

McLean, VA 22102

703-570-8010 | SBritt@BerenzweigLaw.com | www.BerenzweigLaw.com