

Cybersecurity for In-House Counsel: Achieving Compliance (and Beyond) in a Breach-A-Day World

David G. Ries

John L. Hines, Jr.

Linda M. Watson

October 19, 2016

Clarkhill.com



CLARK HILL

David G. Ries

Pittsburgh, PA

412-394.7787

dries@clarkhill.com



John L. Hines, Jr.

Chicago, IL

312.985.5927

jhines@clarkhill.com



Linda M. Watson

Birmingham, MI

248.988.5881

lwatson@clarkhill.com



www.clarkhill.com/contents/cybersecurity-data-protection-privacy

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

FBI Director Robert Mueller
RSA Cybersecurity Conference
March 2012



THREAT ACTORS

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



ATTACK VECTORS

- Direct attack
- Watering hole attack
- DNS compromise
- Phishing / social engineering
- Malware / crimeware / ransomware
- Misuse of admin tools
- Infected devices
- Denial of service
- Supply chain attack
- Physical theft / loss



WHAT THEY'RE AFTER

- Money
- Personally identifiable information
- Intellectual property
- Trade secrets
- Information on litigation & transactions
- Computing power
- National security data
- Deny / disrupt service +

"... because that's where the money is."



MARCH 2016 - FBI WARNINGS

Criminal seeks hacker to break into international law firms



4 March 2016

Alert Number
160304-001

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

“Criminal-Seeking-Hacker” Requests Network Breach for Insider Trading Operation

Summary

A financially motivated cyber crime insider trading scheme targets international law firm information used to facilitate business ventures. The scheme involves a hacker compromising the law firm’s computer networks and monitoring them for material, non-public information (MNPI)¹. This information, gained prior to a public announcement, is then used by a criminal with international stock market expertise to strategically place bids and generate a monetary profit.

APRIL 2016 - CEO E-MAIL SCHEMES

- Oct 2013 through Feb 2016 - 17,642 victims
- More than \$2.3 billion in losses



MARCH 2016 - W-2 PHISHING SCHEMES

Proskauer Rose + Snapchat + Seagate +++



The screenshot shows the IRS website interface. At the top left is the IRS logo. To the right are links for "Subscriptions" and "Lang". Below these is a search bar. A navigation bar contains links for "Filing", "Payments", "Refunds", "Credits & Deductions", "News & Events", "Forms & Pubs", and "Help & Res". The main content area features a "News Essentials" sidebar with links like "What's Hot", "News Releases", and "IRS - The Basics". The main article is titled "IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s" and is dated "IR-2016-34, March 1, 2016". The article text states that the IRS issued an alert to payroll and HR professionals about a phishing email scheme that purports to be from company executives and requests personal information on employees. It mentions that the IRS has learned this scheme is part of a surge in phishing emails and has already claimed several victims as payroll and HR offices mistakenly email payroll data including Forms W-2. A quote from IRS Commissioner John Koskinen is included, warning that if a CEO appears to be emailing for a list of company employees, it should be checked out before responding.

IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s

IR-2016-34, March 1, 2016

WASHINGTON — The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.

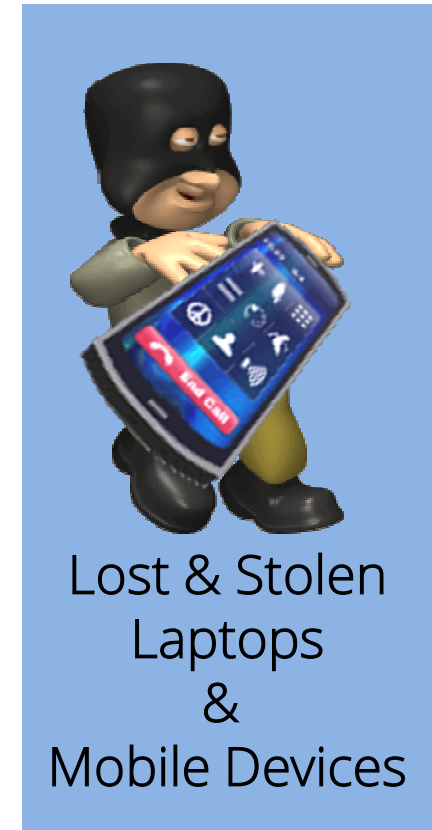
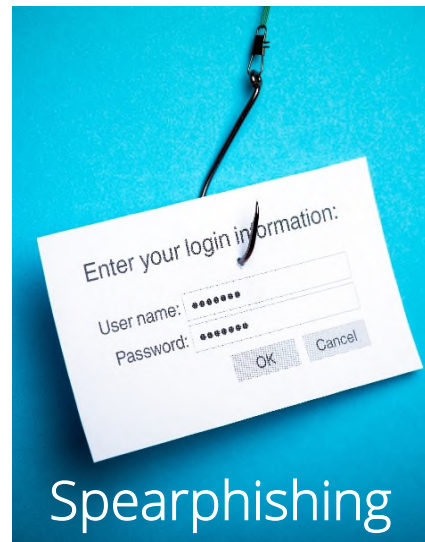
The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

"This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

TODAY'S GREATEST THREATS



Ransomware is a form of malware that targets both human and technical weaknesses in organizations in an effort to deny the availability of critical data and/or systems. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor purportedly provides an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a critical preventative measure.



SECURITY STARTS AT THE TOP

- Board
- CEO / GC / C-level executives
- Establish & maintain cybersecurity program
- Provide budget & authority
- Assign responsibility
- Set the tone



INFORMATION SECURITY

Process



People

Policies & Procedures

Technology



INFORMATION SECURITY

Protect

Confidentiality

Integrity

Availability

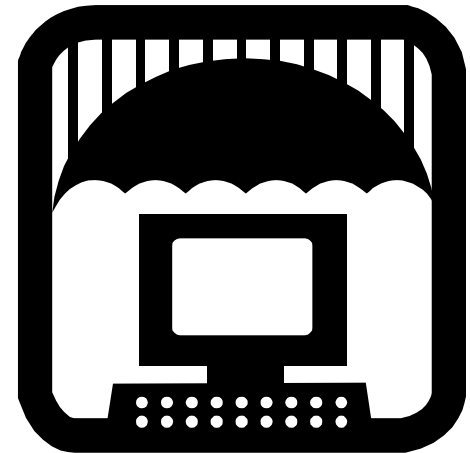


INFORMATION SECURITY

Comprehensive Information Security Program

- Risk-based
- Policies
- Training
- Review and update

Constant security awareness



NIST CYBERSECURITY FRAMEWORK

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014



STANDARDS / FRAMEWORKS / CONTROLS

- NIST *Framework*
- NIST Special Publication 800-53, Rev 4
 - + numerous additional standards
- ISO/IEC 27000 series standards:
 - Information Security Management Systems
- ISACA - COBIT
- Center for Internet Security
- *CIS Controls for Effective Cyber Defense Version 6.1*

STANDARDS AND FRAMEWORKS

Small Businesses:

- NIST's *Small Business Information Security: The Fundamentals, Draft NISTR 7621, Rev. 1* (30 pages)
- U.S.-CERT: resources for SMBs



RISK ASSESSMENT

1. Identity Information Assets
(data, software, hardware, appliances and infrastructure)
2. Classify Information Assets
3. Identify Security Requirements
(statutes and regulations, contracts, common law, "reasonable security," business needs)
4. Identify Risks

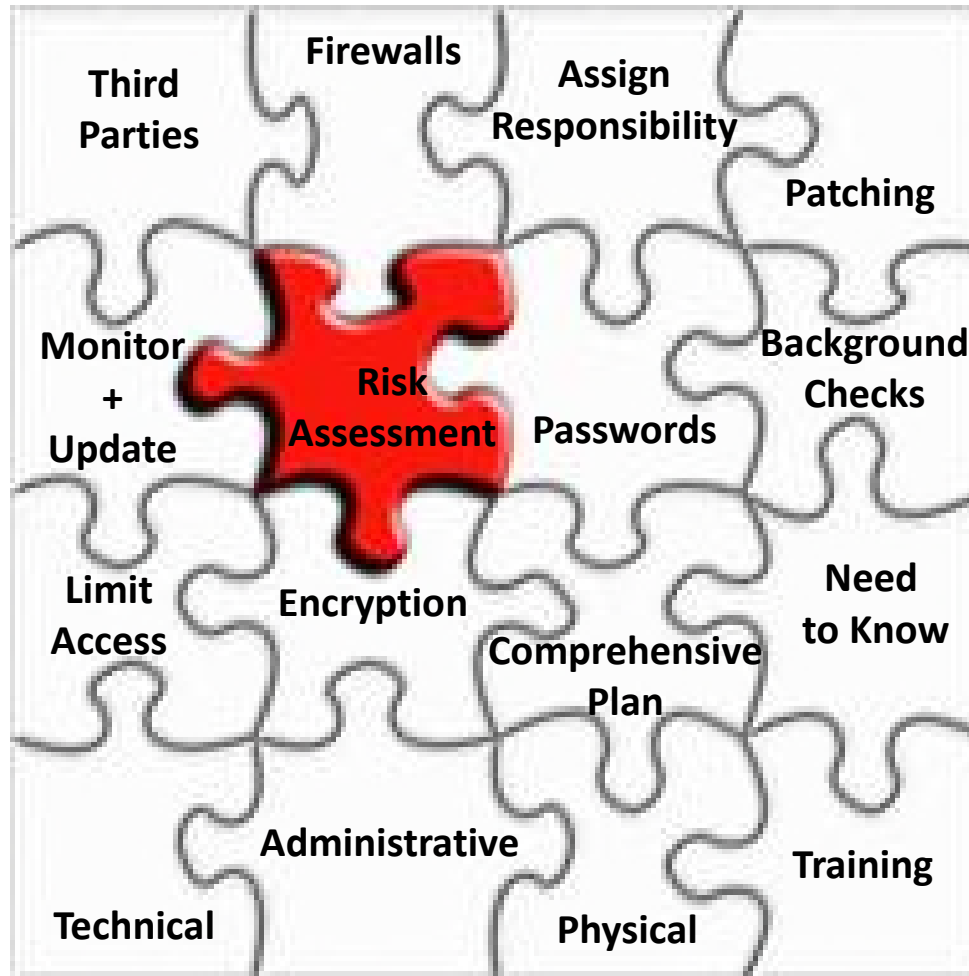


MANAGING RISK

1. Apply security policies and controls to manage the risk
2. Transfer the risk (insurance / contracts)
3. Eliminate the risk
4. Accept the risk



SECURITY REQUIREMENTS



[illegible]

INCIDENT RESPONSE PLANS

Preparing for when a business will be breached, not if it may be breached

The new mantra in security:

Identify & Protect + Detect, Respond & Recover



SECURITY IN TECH CONTRACTS

1. What kind of contracts?
2. What does security in K mean?
3. Absence in K may be violation of law
4. Negotiating security terms



SECURITY IN M&A

Is your organization positioned for M&A due diligence?



QUESTIONS?

David G. Ries

Pittsburgh, PA

412-394.7787

dries@clarkhill.com



John L. Hines, Jr.

Chicago, IL

312.985.5927

jhines@clarkhill.com



Linda M. Watson

Birmingham, MI

248.988.5881

lwatson@clarkhill.com



THANK YOU

Legal Disclaimer: This document is not intended to give legal advice. It is comprised of general information. Companies facing specific issues should seek the assistance of an attorney.



CLARK HILL