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 +





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 +++



Subscriptions V Lang

Search

Filing

Payments

Refunds

Credits & Deductions

News & Events

Forms & Pubs

Help & Res

News Essentials

- · What's Hot
- News Releases
- · IRS The Basics
- IRS Guidance
- Media Contacts
- · Facts & Figures
- Around the Nation
- · e-News Subscriptions

The Newsroom Topics

- · Multimedia Center
- · Noticias en Español
- Radio PSAs
- Tax Scams
- · The Tax Gap
- Fact Sheets

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



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 regalan 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

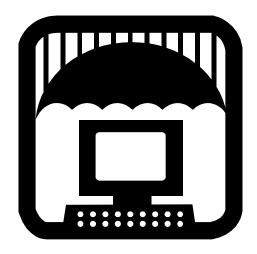
Availability

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

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

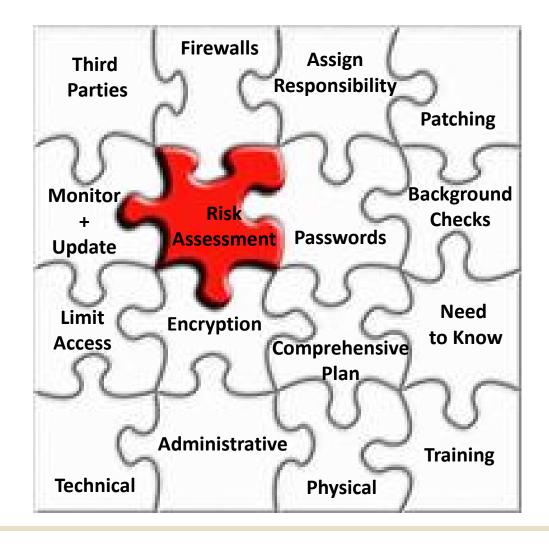


MANAGING RISK

- 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



MAPPINGS TO THE CIS Critical Security Controls Claud FYIS FISHA 2011 NIST Care DHS CDM 850 150 Framework Program 27002-2013 27002-2005 UK Cyber Essentials FFEEC Examiners Handbook HERC CIP vs HERC CIP vs NSA Top 10 - MAID Plange Fearing - 1986 House Sensity Service Inventory of Authorized & Unauthorized Devices EDAN) EDAN) ELEC the leastly - SESTED Notation for 1. - SESTED Retailed States -Ver Epiperer Serving (Mekstein, Laphy, Randinia) 1001 Faring Asset OLT CHA BA DA OLZ CHAR ICAS PRO Facilie Mangineri Treatable Facility Name Name Treatable and Owner Panagement fee Hearty Inventory of Authorized II. - Assistin Writing - WELL Though Stanfo 2 & Unauthorized Software BAN2 BAN4 - SALDROS Newscare for A 1,716 - 144 Differ Materials Towers . · 2005 Steam Season See OF RIE + Gelei Ministrale Pringe + Se a heart Rador Geograph AHDA AHDA AHDA Det Harry 3 Secure Configurations for Handware & Software · Just Configuration · Falls Faragement jetrg: Respond - Ma Montage of Miles - IREDUCTORANIA Source - B 14 th Planer Leaf-gradies edjarder and Despr DAY DAY - TUNINGS Youth Panagement Ing Management Institution and Change Management Feet House 291854 M 291824 M 291824 M CPART I M CPART I M CPART I M Continuous Vulnerability DET MAR DA ARAD + life Minnings of Software Improvements - 144,518bit Noderman Ros. A. - 1941): House Steeler Fact Response - Latine Collect AH/3 A HEAR · ULTRICKSON FOR - F MINI Sunge Swarty Service | IP 478 | 10 + Geologischer et III and TU CHARLE COMPANY OF CHARLE OF CHARLES OF CHARL 5 Controlled Use of Administrative Privileges 18-81 - 18-11 · SECURIT MANAGED SORRY - B Maintenance, Monitoring. DESCRIPTION - Leave falls DESCRIPTION | Name of Street Interested Interested Entrepresent AUGS - AGAS . 164.188(sql); Severy Paragement Prenss - Information System Astering Review 1 - 87117 Phases Sender (%)-80 (%)-80 · Tay Management ionly funera TRADLE M 6 & Analysis of Audit Logs DAT THE DATE CHIEF DATE THE DATE CHIEF DATE THE DATE THE Facility Resignant Hustins Management Tapanot Best Protinces - ATTIT Though Heavier Enal & Web Browser AHEA AHEE AHEE First Interth 1.5 • Set a Secure Standier Geologistics 31 • May Admittage of Settings DEADER OF the Copper leads (Notation Lights & the Mestage of Settage - Park Bargeres - MURRY Retries Sonry - E SPAIR I MIT Flogs Ladgestic 7 34 - the desidence file Aspensaries 17 18 - Ingile Anti-Dalategale Pental - New Yorks + MSS Rough Searth Street City 18.7 S.AV S.A 16.07 S.7 S.4 A1881 - \$15.67 RO-IS TENE 8 Halware Defenses IE ON A SP-863-4-81 DEMOTE N A187.1 - Bubb bei Egbergten Sotore 9 Limitation & Control of Network Ports Interested Security Encaptures ATEA - Enter Register ATEA - Subprise of Deep Register 1 II - Smit Workspin in Weltpales Generalizati + #FETT Haupt Searty (F) (E) PLACE TEACH busing frame Street Interly Rosel South SPARTS N BF487.) (2) - III) By Brigge Very - I MIN Samp Source Service HAJRAGES Gestegeng Plan - Dem Ferling Plan B HAJRAGES Gestegeng Plan - Gestege Augment Plan B HAJRAGES Gestegeng Plan - Festing & Lection Procedure A HAJRAGES Berling & Rock Gested - Juna Noting & Houge & AIRE) - PRIT Place South Data Recovery Capability MF4 NS-II AIRES - AIRES - May for female Jeanty Gatespe, frame and Ferredi #211 Haup Searty Secure Configurations for Network Devices + Se a Seas Rades Conference Configuration and Change Rangement Book hory MIN Rough Sweety Service + ligger femon oil factor Hill Street Columbus - Nemali Seletation - Resides Paragraphi 16-11 18-12 PLACE PLACE PLEGAL PLACE 2 Boundary Defense Impropriate Louises for Transmig Date 17-10-1 12 Senior . Goldy Sentral Hill Street States level **19 MT4 M** DE METER NE irati u · Named Traver I Sensory Trends M.1 (3-5 KA E-4 MA B.5 E-26 M.11 NOT NOT A10.17 - A10.13 A10.21 - A10.22 - Devis Academics HARDAY I virence kora Response, inhitig held her Dempless Resides (HARDAY) met und Suita Conner - According A HARDAY) band don't "Banday or de Polygian A HARDAY | Banday or de Polygian A 3 Data Protection Tearty Existing: Proof, and Sensit: Sensiti Tearty Restring - Date Coming 1935 Sings Sensity Serve

AL-0 102-01 AL-0 102-01 AL-04 76-04 III-03 AULI AULIA AULI A10.4 A10.0 A10.0 A10.0 A10.04 lifeen Smilgmen & Aspection . 2001 States Swarty Swiss CR CR CR 9 Incident Response & Management 82 84 87 82 84 84 83 84 84 - Plat for Freit (\$F-200.4 K) (SPARE) IL (1.19 - 164.185)((1) Jeansy builder, Provident - Name and Asserting & DRAME I AV 1941 - 1945 | frieder legen (PAN) IS - AFRIC Plane Leady - Hill Mange leastly leader. 20 Penetration Tests 264 E64 P64 264 E64 P644 Identification Streety Suspensed AREA AREA AREA CIS CRITICAL SECURITY CONTROLS

0.6

tanging for Invites Report Fearing

4711 4827 - Tubbe

 Formal Bureni: Beri Paragenera
 Bernert Sone Corps



19-80-4 65 19-80-5 65 29-80-4 61

COMMAND.

27-101-4 17

DF-894 4 KI

0640116

ERABE F BE

29-800-F N

Hitt. Sang Journ Terrior

· Whit them have

· #40 Base Issuits

1000 Rose Senty Invest 19404 | KJ

 OH PERSON Processor Study - Inagely Sector A
 OH PERSON Supposed Sector - Desper

"HUMBASS") Energy bearwast and bezong - Scorey beronders A
 "HUMBASS" Securey bearwast and bezong - Scorey beronders A
 "HUMBASS" Securey bearwast and bezong - Secure Bost Bearbass Secure A
 "HUMBASS" Securey bearwast and bezong - bearwast broughouse A
 "HUMBASS" Securey bearwast and bezong - bearward broughouse A

Data South

Ecoption Security Besturing DP485-7 KE DP486-7 KE DP486-7 KE

OHERS IS

DEADLE BY

DEADLE IN

CHANGE IS

OF 4943 ID

15-40 75-48 865-11

100-10 100-65 Interior Swapter

4 Controlled Access Based on the Need to Know

5 Wireless Access Control

6 Account Manitoring

7 and Appropriate Training to fill Gaps PLACE PLACE PLEFE

MUGIL MUGIL MUGIL MUGIL MUGIL

#1 #4 Mil #2 #11 Mil #4 #10 Mil

INCIDENT RESPONSE PLANS

Preparing for <u>when</u> a business will be breached, not <u>if</u> 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.



