Cybersecurity and HR Records

Cami L. Davis  
(412) 394-2357  
cdavis@clarkhill.com

David G. Ries  
(412) 394-7787  
dries@clarkhill.com
TODAY’S PRESENTERS

Cami L. Davis  
(412) 394-2357  
cdavis@clarkhill.com

David G. Ries  
(412) 394-7787  
dries@clarkhill.com

clarkhill.com/contents/labor-employment-law  
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
THE INSIDE THREAT

- Malicious
- Disgruntled
- Untrained
- Careless
- Rogue technology
- Bored
- Lost / stolen devices
- Departing employees
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.”
HR AND PAYROLL ARE TARGETS!

$\ldots$
Tax Fraud
Identity Theft
IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments

IR-2017-10, Jan. 25, 2017

WASHINGTON – The Internal Revenue Service, state tax agencies and the tax industry today renewed their warning about an email scam that uses a corporate officer’s name to request employee Forms W-2 from company payroll or human resources departments.

This week, the IRS already has received new notifications that the email scam is making its way across the nation for a second time. The IRS urges company payroll officials to double check any executive-level or unusual requests for lists of Forms W-2 or Social Security numbers.

The W-2 scam first appeared last year. Cybercriminals tricked payroll and human resource officials into disclosing employee names, SSNs and income information. The thieves then attempted to file fraudulent tax returns for tax refunds.
WASHINGTON — The Internal Revenue Service, state tax agencies and the tax industry issued an urgent alert today to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits.

In a related development, the W-2 scammers are coupling their efforts to steal employee W-2 information with an older scheme on wire transfers that is victimizing some organizations twice.

“This is one of the most dangerous email phishing scams we’ve seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone’s help to turn the tide against this scheme,” said IRS Commissioner John Koskinen.

When employers report W-2 thefts immediately to the IRS, the agency can take steps to help protect employees from tax-related identity theft. The IRS, state tax agencies and the tax industry, working together as the Security Summit, have enacted numerous safeguards in 2016 and 2017 to identify fraudulent returns filed through scams like this. As the Summit partners make progress, cybercriminals need more data to mimic real tax returns.
W-2 PHISHING SCHEMES

“Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.”

“Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).”

“I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.”

Cloudmark Security Blog
SPEARPHISHING + WHALING

- Company Websites
- Internet Searches
- News Releases
- Biographies
TODAY’S GREATEST THREATS

Ransomware

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.

Spearphishing

Lost & Stolen Laptops & Mobile Devices
INFORMATION GOVERNANCE

www.edrm.net
Security
Privacy
SAFEGUARDING CONFIDENTIAL INFORMATION

- Laws and regulations
- Common law
- Contracts
- Protecting brand and reputation
- Employee relations
SECURITY STARTS AT THE TOP

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

- Board
- CEO / GC / C-level executives
- Management
- IT
- HR
- Risk Management
- Finance and Accounting
- Marketing
- Records and Information Management
- Business Units EVERYONE
INFORMATION SECURITY

Process

People
Policies & Procedures
Technology
INFORMATION SECURITY

Protect

Confidentiality
Integrity
Availability
INFORMATION SECURITY

Comprehensive Information Security Program

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

Constant security awareness
HR’S ROLE IN SECURITY

- Participate in developing, implementing and maintaining the organization’s comprehensive information security program
- Training
- Enforcement: counseling and discipline
- **Safeguarding HR records**
  - Dealing with employees during incident response
  - Assisting employees whose PII has been compromised
  - Dealing with departing employees
MONITORING EMPLOYEES

- Policy
- Consent
- Monitoring tools
- Data loss prevention (DLP)
STANDARDS / FRAMEWORKS / CONTROLS

- NIST Framework
- NIST Special Publication 800-53, Rev 4 + numerous additional standards
- ISACA - COBIT
- Center for Internet Security
- CIS Controls for Effective Cyber Defense Version 6.1
NIST CYBERSECURITY FRAMEWORK

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0
National Institute of Standards and Technology
February 12, 2014

Draft Version 1.1 released Jan. 2017
STANDARDS AND FRAMEWORKS

Small Businesses

- NIST's *Small Business Information Security: The Fundamentals, NISTR 7621, Rev. 1* (32 pages + appendices)

- 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**
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*
BREACH NOTICE LAWS

State

- 48 states

Federal

- Gramm-Leach-Bliley - regulations
- HIPAA – law & regulations
- Veterans
Report identity theft and get a recovery plan

Get Started

IdentityTheft.gov can help you report and recover from identity theft.

**HERE’S HOW IT WORKS:**

1. **Tell us what happened.**
   - We’ll ask some questions about your situation. Tell us as much as you can.

2. **Get a recovery plan.**
   - We’ll use that info to create a personal recovery plan.

3. **Put your plan into action.**
   - If you create an account, we’ll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
“THE GOOD OLD DAYS”
REMOTE ACCESS

Corporate Network

Encrypted Communication Channel

Internet

Strong Authentication

VPN HTTPS

Remote User
CLOUD SERVICES

Corporate Network

Strong Authentication

Internet

ERP / ERM / HRM / HCM

Encrypted Communication Channel
ENCRYPTION OF DOCUMENTS

- Microsoft Office
- Adobe Acrobat
- WinZip

Limited Protection!
SOME TAKEAWAYS

- **Encrypt** laptops, smartphones, tablets and portable media
  
  Verizon Enterprise: “As close to a no-brainer solution as it gets.” “Just do it.”

- **Encrypt** confidential data sent by e-mail or over the Internet
  
  Bruce Schneier / CERT/Google: “unencrypted e-mail is like a postcard”

- **Provide** ongoing training
  
  Users are often the weakest link

- **Promote constant** security awareness
  
  ... by every user, every time they’re using technology
QUESTIONS?

Cami L. Davis
(412) 394-2357
cdavis@clarkhill.com

David G. Ries
(412) 394-7787
dries@clarkhill.com

clarkhill.com/contents/labor-employment-law
clarkhill.com/contents/cybersecurity-data-protection-privacy
THANK YOU

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