Taming the Monster in the Machine: Engaging Your Employees in the Battle Against Cyber Threats

Presented by:
Kerin E. Stackpole, Esq., SPHR
Paul Frank + Collins P.C.
KERIN E. STACKPOLE, ESQ., SPHR

Kerin E. Stackpole is a Director at Paul Frank + Collins P.C., where her practice areas include employment law, business counseling and general civil litigation. A native of Burlington, Vermont, Kerin is admitted to practice law in Vermont, Maryland and the District of Columbia. Kerin is an honors graduate of the Washington College of Law, American University and of Wheaton College, Norton, Massachusetts. Before returning to Vermont, Kerin practiced law in Washington, D.C., concentrating in employment and business law. She has been involved in litigation on a wide range of employment and business law issues. In addition to practicing law, Kerin also teaches. She has taught at the law schools of Catholic University of America, The American University, as well as at the University of Vermont and Champlain College. She has also lectured at Georgetown University’s law school. She also regularly designs and presents training programs for businesses and management personnel on employment law issues. Kerin was the Chair of the Employment Law Section of the Vermont Bar Association from 2000 until 2004 and in 2008 she received her certification as a Senior Professional in Human Resources. Since 2009, Kerin was recognized as one of Vermont’s top labor and employment attorneys by Chambers & Partners (USA); and since 2011 she was also recognized by her peers for achievement in employment and labor law by Best Lawyers of America.

NOTE TO READER

The information contained herein is based upon sources believed to be accurate and reliable – including secondary sources. While we have exercised reasonable care to ensure the accuracy of the information contained here, no representation or warranty is made as to such accuracy. Readers should check primary sources where appropriate and use traditional legal research techniques to make sure that the information has not been affected or changed by recent developments.

The paper is presented with the understanding that the author does not render any legal, accounting, or other professional service. Due to the rapidly changing nature of the law, information contained in this paper may become outdated. In no event will the author be liable for any direct, indirect, consequential or other damages resulting from and/or related use of this material.
Taming the Monster in the Machine: Engaging Your Employees in the Battle Against Cyber Threats

Presented by Kerin E. Stackpole, Esq. and Kristina R. Brines, Esq.
Paul Frank + Collins PC.

© 2016 Paul Frank + Collins P.C. All Rights Reserved.

No One Is Safe

- So far in 2016, there have been approximately 378 reported data breaches in the United States and more than 11.53 million records have been stolen.

- 45% were in the business sector and 34% of these breaches have occurred in the health care industry.

No One Is Safe

- Most breaches are caused by external actors, primarily for financial gain.

- Installation of Malware and Hacking through the use of stolen credentials/information are the two most common types of breaches.

- Most hackers use phishing emails (emails that look real, but are not) and attacks on POS (point of sale) devices. Source: Verizon 2016 Breach Investigations Report.

On May 4, 2016, ADP, the payroll processing company, was hit by a cyber attack.

- U.S. Bancorp, one of ADP’s clients, had tax and salary data stolen for about 2% of its 67,000 employees.

- Thieves apparently used names, addresses, and dates of birth stolen in a previous incident that hit U.S. Bancorp directly, to access ADP information in their names.

No One Is Safe

- Possessing previously stolen identifying information enabled hackers to “walk through ADP's front door” because they already had information about the individual.

- W-2 data allows thieves to file fraudulent tax returns to get your refund, and allows them to apply for credit in your name.


No One Is Safe

ADP serves more than 630,000 clients worldwide.

Cybersecurity – protection of information and systems
- Can refer to computer apps, programs or platforms;
- Can refer to processes and policies

Incident: A security event that compromises the integrity of a company’s systems or info

Breach: Personally identifying information, such as names, SSNs, addresses, etc., is actually taken by a third party.

Protected Health Information (PHI)
- HIPAA/HITECH
- Patient Data

Payment Card Industry (PCI)
- Credit Card Data

Personally Identifiable Information (PII)
- Privacy Act of 1974
- Vermont law
- Name, Address, SSN, DOB

Sensitive Information (trade secrets, financial, legal, etc.)
- Payroll, W-2, Budget, corporate strategy, etc.
Understanding the Jargon

- TRADE SECRET – has particular definitions under state and federal laws, but essentially:
  - Proprietary information of the company, including things like formulas, patterns, compilations, programs, devices, methods, techniques and processes.
  - Can include customer lists
  - Is subject to scrutiny re an employer’s efforts to maintain secrecy.

Understanding the Jargon

- Proving something is a “trade secret” requires more than just showing it was “confidential.” It will likely require a showing of:
  - Independent economic value (actual or potential)
  - That the employer made reasonable efforts to keep it secret
  - That the info is not readily ascertainable by proper means, and
  - Is not available publicly
By the Numbers

2016 Percentage of Breaches By Industry Type

- Banking/Credit/Financial
- Business
- Educational
- Government/Military
- Medical/Healthcare

(source: 2016 Identity Theft Resource Center)
By the Numbers

- A 2013 report by the Commission on the Theft of American Intellectual Property found the following:
  - IP theft through cyber hacking causes American businesses approximately $300 billion in losses – annually.
  - In 2013, 50–80% of losses were attributed to people located in China and/or the Chinese Government (but we are now seeing local attacks more and more frequently).
- The Justice Department attributes the loss of more than 2 million jobs at American companies to corporate espionage.
- The Commander of the U.S. Cyber Command and Director of the National Security Agency has called IP theft in recent years “the greatest transfer of wealth in history.”

The Human Element

- 1 in 5 North American employees keep passwords in plain sight
- 1 in 3 cloud app users have downloaded an app without ever telling their IT department
- 44% of employees have not been told how to securely transfer or store private corporate data
- 58% of FT employees say they have never been trained on how to download or use cloud apps
- 23% of cloud app users claim there is a popular app that employees use that is not supported by IT (e.g. Dropbox or Google Docs)

Source: Softchoice Cloud Computing Survey 2014
The Human Element

- 1 in 4 employees manages passwords in a doc that is not itself password protected.
- 1 in 5 employees accesses work files from a device that is not password protected.
- 1 in 5 employees has lost a device that was not password protected.

Source: Softchoice Cloud Computing Survey 2014

Generational Differences

- 31% of Millennial employees surveyed downloaded cloud apps without letting IT know, as compared to 30% Xers and only 22% of Boomers.
- Most common motivation: IT is too slow to approve their choice!

- 22% of Millennials have downloaded unsanctioned apps even if IT offers an approved version, compared to 13% of Boomers.
- Most common motivation: IT’s version does not improve productivity or lack of compatibility across devices.

Source: Softchoice Cloud Computing Survey 2014
Generational Differences

- 30% of Millennial employees have accessed work files through an app IT does not know about.
- Compare this to 27% of X’ers and only 12% of Boomers.

Motivations: Easier access; better compatibility across devices.

Source: Softchoice Cloud Computing Survey 2014

Risks in the Cloud

Cloud app users are 2x more likely to:

- Keep passwords on post it notes.
- Store passwords in an unprotected shared drive.
- Manage passwords in an unprotected document.
- Access work files from an unprotected device.
- Lose a device with access to work files on it.

Source: Softchoice Cloud Computing Survey 2014
Data Every Employee Needs to Protect

What Sort of Data Should You Be Protecting?

- Credit Card info
- Social Security Numbers
- Financial Information
- Passwords
- Trade Secrets
- Any sensitive data that someone might not want to fall into the wrong hands
Whose Data Should You Be Protecting?

- Company Data
- Consumers’ Data
- Employees’ Data
- Client or patient data (holding their data for their use – storage, payroll, legal, etc.)

Every Employee is Part of the Solution
Teach Employees the Basics
Source: Identity Theft Resource Center

- **Strengthen passwords**
  - Use at least 8 characters, alpha numerics, symbols and upper/lower case

- **Handle PII with care**
  - Don’t give out Personal Identifying Information (PII) unless absolutely necessary

- **Read credit reports annually**
  - Go to AnnualCreditReport.com for a free credit report annually

- **Empty your purse/wallet**
  - Don’t carry any more than necessary and never your Social Security card

- **Discuss these tips with friends**
  - Share your knowledge and educate those around you

---

The Basics of Phishing

- Email filtering – use a spam or other type of filter that requires employees to make choices about what should be permitted and what should not.

- Teach employees about Phishing
  - What does a phishing email look like?
  - What are the telltale signs?
  - What do you do if you get one of these?
    - Don’t just delete it – BLOCK IT
    - Tell IT about it; tell other employees you got it and it is phony.
Prevention Methods

- Conduct tests – send an internally generated phishing email, to see who bites.
- Follow up with employees who fall for your internal phishing tests and have them get more training.
- Segment your network/systems and create firewalls between emails and information you need to protect.
- Implement strong authentication protocols to get into files and programs containing sensitive information (e.g. more than one consent needed to provide PII, PHI, PCI or Sensitive Information).

- Monitor “outbound traffic” for suspicious connections and potential “exfiltration” of data.
- Have a very specific policy requiring employees to report phishing emails and accidental breaches. (“Oops, I clicked on it…”)
- Make reporting breaches easy and part of every employee’s responsibility.
HR and IT Working Together

- Perform a Cyber Security SWOT Analysis and engage managers and key employees.

- Create policies relating to cyber security priorities and goals.

- Create specific procedures for:
  - Employee access to technology
  - Protecting company issued devices and information
  - Protecting company information on personal devices
  - Reporting incidents and breaches
  - Reporting violations of policy that put data at risk
Training and Communication are Key to Cyber Security

- HR and IT need to partner in engaging employees as front line defenders.

- Regular Discussions of Employee Obligations, Protocols, Successes and Failures:
  - At Orientation
  - A Regular, Periodic Training Sessions
  - At Team Huddles or Department meetings
  - Interoffice newsletters

- Celebrate and publicize successful employee actions that helped protect information/data.

- Use “near misses” or actual incidents as teaching tools.

HR and IT Working Together

- Working with HR, IT should periodically survey employee behaviors and preferences.
  - What is working? What could be improved?
  - What have employees seen in the industry?
  - Are there other or newer devices out there?
  - Are there other apps or platforms that can improve productivity, connectivity, or user experience?

- Conduct periodic audits of work-related devices, programs, policies and processes – to assess compliance and vulnerabilities.

- Engage with employees as to why they may stray from using sanctioned apps or proper procurement procedures.
Training and Communication are Key to Cyber Security

- Anticipate that some employees may want to use popular consumer apps with which they are more familiar.

- Get ahead of them with information on dangers of such apps and virtues of apps IT has vetted.
  ◦ Don't download free apps without checking with IT first.
  ◦ Continually train on apps or programs that the company has approved, so employees get more comfortable with them.

IT and HR Working Together

- Create and periodically publish a “safe list” of apps that have been vetted.

- Coordinate and control access to vetted apps. For example: create access from one location on the company’s system; or have a process for getting them downloaded through a centralized “help desk” or other provider.

- The Company needs access to passwords to key programs and/or devices.
Developing Policies that Work

Developing Cyber Security Policies and Practices

• Identify potential reputation and business risks associated with a breach
  • Communicate these risks to employees
  • Communicate costs and consequences to employees

• Establish security roles & responsibilities and communicate them regularly
  • Senior Leadership
  • Management
  • Every Employee
Developing Cyber Security Policies and Practices

- Identify personal data v. business data.

- Carefully consider use of company or business devices

- Lower Expectations of Privacy for Employees
  - Establish company’s right to monitor, examine, block or restrict access.

- Consider requirement for separate Non-Disclosure Agreement that all employees are required to execute during employment.

  - Independently enforceable.
  - Provides explicit notice of information to be protected.
  - Includes Trade Secrets and other important data, processes, assignment of rights to inventions, new processes, etc.
Developing Cyber Security Policies and Practices

- Let employees know that all data/communications (even “personal” communications) may be “discoverable” in litigation.
  - Sexual harassment suits
  - Trade secret actions
  - Enforcement suits re restrictive covenants
- Periodically monitor internet use of employees and remind them that you are doing it.

Developing Cyber Security Policies and Practices

- Have a policy addressing Internet Use and potential monitoring.
- Establish social media guidelines (consider Section 7 of NLRA and its implications)
- Have a policy that limits “updates,” and installation of software to IT only.
- Create information and device retention and/or disposal process.
What If There Is a Breach? What Do You Do Now?

What Employers Need to Know in the Event of a Breach

- In which states does the organization conduct business?

- What are the requirements in each state for reporting a data breach or protecting privacy of customers or employees?

- What constitutes a data breach in those states?
What Employers Need to Know in the Event of a Breach

- What are the reporting requirements?

- What safe harbor clauses are allowed under these state laws?
  - For example, most of the state laws allow for an encryption safe harbor, which means that if the breached data is encrypted, reporting is not required or the reporting requirements are minimized significantly.

Vermont’s Security Breach Notice Act

- 9 V.S.A. § 2430 and § 2435

- Applies to Businesses and State Agencies
  - Enforced by either AG or DFR (was BISHCA)
  - Does Not Apply to Certain Financial Institutions

- Applies to Loss of “Personally Identifiable Information”

- Amended Effective May 8, 2012
What is Personally Identifiable Information (PII) under Vermont Law?

First Name or First Initial & Last Name (if it has not been encrypted or rendered unreadable), AND
- Social Security number; OR
- Motor vehicle operator’s license number or non-driver identification card number; OR
- Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; OR
- Account passwords or personal identification numbers or other access codes for a financial account.

Definition of “Security Breach” under Vermont Law

“unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer’s personally identifiable information maintained by the data collector.”
Definition of “Security Breach”

“does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.”

Factors to consider when determining if a breach has occurred:

(i) Information is in someone else’s physical custody (i.e. stolen laptop);
(ii) Information has been downloaded or copied (i.e. hacking, malware, unauthorized use);
(iii) Information has been used by an unauthorized person (i.e. reports of fraudulent accounts opened or ID Theft); or
(iv) that the information has been made public.
You Think You Have Had a Breach...What do you do?

1. Secure Your Data
2. Investigate How It Happened
3. Notify your Insurance Carrier, as applicable
4. Contact Law Enforcement
5. Contact Entities From Which You Obtained the Data
6. Notify the Attorney General’s Office Of The Breach within time required by law
7. Notify Consumers Of The Breach, as required by law
8. Notify the Credit Reporting Agencies (if more than 1,000 consumers)

Contact Law Enforcement

1. Call the FBI, Secret Service
2. Inform Them Of Your Duty To Notify Customers
3. Determine Whether Law Enforcement Wants You To Delay Notification
Timing of Notice Requirements

1. All Notices Should Go Out In The Most Expedient Time Possible
2. 14 Day Preliminary Notice to AG (non-public)
3. Final Notice to AG and to Customers (public) within 45 days
4. May only be delayed on request from law enforcement

Contents of Notice Requirements

- Incident in general terms.
- Type of PII accessed
- General acts taken to protect the PII from further breaches
- Telephone number, toll-free if available, for further information.
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
- The approximate date of the security breach.
Manner of Notice Requirements

- Direct Notice
  - Mail
  - Email (if requirements are met)
  - Telephone (not prerecorded)

- Substitute Notice (Website and Major Media)
  - If cost would exceed $5,000 to send direct notice
  - If number of customers exceeds 5,000
  - If insufficient contact information

No Harm Letter

- Notice Not Required if Misuse of Personal Information is Not Reasonably Possible

- Notice of this determination with detailed explanation sent to Vermont Attorney General
Penalty for Noncompliance under Vermont Law

- Violation of the Consumer Protection Act
- $10,000 Civil Penalty per Violation
- Violation = Customer Not Noticed Per Day

Key Takeaways

- Every employee needs to know that he/she has a responsibility in the battle against cyber attacks.
  - Communicate, Communicate, Communicate

- Every employee needs the training to fulfill this responsibility.

- Create and update good policies.

- Conduct audits of use and compliance periodically.
  - Make sure employees have what they need and how to use it.
Key Takeaways

- Encourage (and require) employees to report actual or suspected breaches.
  - Forgive innocent mistakes and learn from them.
  - Every mistake is an opportunity for retraining.
  - Carelessness should have consequences.

- Every employee needs to know WHEN to report an actual or suspected breach.

- Create a team to respond to breaches.

Contact Info

- Kristina R. Brines, Esq.
  Paul Frank + Collins P.C.
  kbrines@pfclaw.com
  802–658–2311

- Kerin E. Stackpole, Esq.
  Paul Frank + Collins P.C.
  kstackpole@pfclaw.com
  802–658–2311