Kroll | A Division of DUFF & PHELPS

Snell & Wilmer

Effective BEC and Ransomware Mitigation

Oct 2019

- Jonathan Fairtlough, Managing Director, Cyber Risk, Kroll
- James P. Melendres, Partner and Co-Chair, Cyber Security, Data Protection and Privacy, Snell & Wilmer

Preparation: What Do We Have to Protect?

Data inventory

Do we know what we have? How long are we keeping it? Where are we keeping it? Why are we keeping it? Who has access to it? Has the data been classified? Who is responsible for the data?

Real time

Do we have the ability to inventory our data in real time, and control access?

Verification points

Data inventory/Map, Data classification policy, Data Loss Prevention (DLP) tools, Data Retention policy, Data use policy

Verification methods

Board committee, third party audit

BOARD OVERSIGHT: Keeping data that can expose the company to risk balanced against the cost of loss

Preparation: Who Holds Our Data?

Do third parties hold data?

Cloud Services, Marketing vendors, PCI services, Web hosting providers

Due diligence?

Contractual right to access, Duty to assist, Regular security review

Verification points

Legal review of vendor contacts that hold data, Copies of vendor security assessments

Verification methods

Include 3rd parties in testing; Ask for regular security updates, Onsite inspection of 3rd party

BOARD OVERSIGHT: Ensure that third parties meet the same security standards as the company.

Data and System Backup

Review and verify your back up strategy:

- What systems and data is being backed up?
- How often do backups happen?
- Where is our data back up to?
- How often to we verify the backups?
- How complete is the verification?
- Is a physical copy kept?
- Do we have images of key system data?

- A good backup acts as a last defense- it ensures that if all else fails, the data needed to keep a business running is available. Everyone has one- kind of

- Backup is boring, tedious, consumes disk and It resources, and can sit for years without being needed.

- It can fail for multiple reasons:
- 1. It was not done properly, and no one checked.
- 2. The wrong things were backed up.
- 3. The media failed, and there was no redundancy
- 4. The attacker turned it off, or destroyed it

- Ask your IT team the questions on the side bar.
- Make sure you know the what, where and how of your backups, and test what you are told.

Multi Factor Authentication (MFA)

Do we have MFA installed with the services for:

- Financial controls
- Audit reporting systems
- ERP systems

Do we have MFA installed for email?

- Office 365/ GSuite

Do we have MFA installed on all systems used for remote access?

- VPN?
- Citrix/ VmWare
- FTP

- Username and password is no longer enough. They are too easy to either guess, research, brute force or trick our of a user.
- Multi-factor Authentication is needed.
- This is when a user needs to enter anther piece of information, usually a code, generated from a token or application or text, in addition to their username and password, to get connected to the system or application.

- Proper deployment can stops the usefulness of the most common attacks:
  - Phishing- the attacker does not have the code
  - Social Engineering- asking for the code must be done each time the attacker wants access
  - Hacking- getting into a network does not get you into data

Preparation: Can We Identify a Problem Early?

How have we defined an event or incident?

What data do we have?, Who has access to it?, How is it regulated?

Notification

What are the ways we get notified about incidents?

Verification points

Review and discussion of Incident definition; Periodic review of system alerts, SOC/NOC escalation, Threat or vulnerability report

Verification methods

Audit- internal & third parties

BOARD OVERSIGHT: Review the definition of an incident with management to ensure that focus is directed on the proper business risks

Engage in Endpoint Threat Detection

A key measure of a modern, effective information security program is its ability to rapidly detect **and** effectively respond to an intrusion. Given the widespread use of cloud data, the detection capacity must exist on the desktop

- Identify and flag known bad executables
- Analyze the behavior shown on a computer against attack methods and processes
- Get data from Multiple threat intelligence sources and ‘learn’ IOC.s
- Be able to conduct threat hunting and get identification of threats
- Rapid notification of **validated** threats

Preparation: Is Help Lined Up?

Existing relationships?

With an IR firm?, Crisis PR firm?, Privacy law firm? Law Enforcement?

Existing MSAs?

Verification points

MSA with firms, Participation in local task forces

Verification methods

Board presentation from 3rd party, Board presentations for local LE, Working with them in training and assessment work

BOARD OVERSIGHT: Ensure that resources outside the company are available and compatible with the business units in case of need

Pre Breach Work - Refining the Incident Response Plan

The questions to ask the client and compliance team

Is there an Incident Response (IR) Plan?

- Does it define what an incident is?
- Does it establish a team with decision-making authority?
- Does it define criteria for declaring an incident?
- Does it define criteria for escalation?
- How often is it tested?
- How is it deployed?

Do we have the technical solutions and expertise to detect an incident?

Pre Breach Work - IR Team Vetting

How to evaluate preparedness

Do we have an IR team?

- Who are the key members?
  - » Legal counsel
  - » Senior management
  - » CISO
  - » PCI implementer
  - » Others

Who leads the team?

- Decision-making authority
- Competence
- Familiarity with the Incident Response Plan

What is the team's purpose?

- Reduce business risk to the organization
- Minimize the impact of an incident on the reputation, operations, and finances of the organization if an incident occurs

Are we providing effective support to the IR team?

- Are we providing continuous training to the team and our staff?
- Does the team have access to all business units and groups?
- Does the IR team have access to details about vendor security?
- Has the IR team identified all third party dependencies?

Protecting Incident Response Under Privilege

Assume potential disclosure

- *United States v. Bryan*, 339 U.S. 329(1950):
  - "There is a general duty to give what testimony one is capable of giving, and any exemptions which may exist are distinctly exceptional, being so many derogations from a positive general rule."
- You are required to disclose communications or reports unless an exception applies
- Treat everything as potentially subject to disclosure

Protecting Incident Response Under Privilege

Information generated

- Responding to a cyber event might generate several types of communications or reports that you may want to consider seeking to protect from disclosure

- These include:
  - Assessment of network vulnerabilities
  - Suggestions for improvements of cybersecurity
  - Previous incidents
  - Management knowledge of previous incidents
  - Consumer complaints
  - Proof of negligence
  - Failure to notify of incident
  - Employee error (phishing)

Protecting Incident Response Under Privilege

Disclosure risk

- Goal: Minimize disclosure risk in responding to cyber incident
- Several adverse parties might seek to discover/make public information that a company or its agents generate in response to a cyber incident:
  - Opposing Lawyers
  - Regulators
  - Press

Protecting Incident Response Under Privilege

Opposing lawyers seeking info

1. FTC and State Attorneys General

- Consumer Financial Protection Bureau: prohibits unfair, deceptive, or abusive practices

2. SEC

- Disclosure requirements for public companies

3. Shareholders

- Securities fraud (alleged impact on stock price)
- Derivative actions (alleged breach of fiduciary duties of care or oversight regarding management of cyber risks or adequacy of public reporting)

4. Business parties

- Litigation not common; usually handled via negotiation
- Contract claims (e.g., compliance with law, notification, etc.)
- Other alleged duties (duty of care owing to “special relationship” or statutory obligations)

5. Private plaintiffs

- Tort law (e.g., negligence, invasion of privacy, etc.)
- Statutory (e.g., FCRA, state laws, etc.)
- Contract claims (e.g., customer agreement, privacy policy, etc.)
- Misrepresentation of practices

Protecting Incident Response Under Privilege

Protected information

- Neither federal nor state courts recognize a stand-alone privilege for cybersecurity communications or work product
- Categories of information protected from disclosure:
  - Attorney–client privilege
  - Work product doctrine
- Goal is to keep information generated in Incident Response efforts in these protected categories

Protecting Incident Response Under Privilege

Attorney-client privilege

- Strongest form of protection
- Protects communications between attorneys and clients in seeking and providing legal advice
- May include non-lawyers who are assisting the attorney in representing the client
- Protects
  - Communications between a client and attorney
  - For the purpose of rendering legal advice
  - Made in confidence

Protecting Incident Response Under Privilege

Work product doctrine

- Weaker form of protection
- Protects information
  - prepared in anticipation of litigation
  - by or for a party or its representative
- Might still be subject to disclosure if another party
  - has a substantial need for the information and;
  - cannot get it elsewhere without undue hardship

Protecting Incident Response Under Privilege

Protections applied

Genesco v. Visa, 302 F.R.D. 168 (M.D. Tenn. Mar. 10, 2014)

- Retailer's GC retained cybersecurity consultant.
- Agreement with consultant stated that engagement was "in anticipation of potential litigation and/or legal or regulatory proceedings."
- In litigation, opposing party sought work product of consultant and deposition of consultant and GC.
- Court largely denied discovery requests.

Protecting Incident Response Under Privilege

The danger of implicit waiver

Leibovic v. United Shore Financial Services, LLC, 2017 WL 3704376 (E.D. Mich. Aug. 28, 2017)

- The privilege cannot be used as both "a sword and a shield."
- United Shore disclosed the conclusions from its forensic firm's reports, but asserted work product protection over the reports.
- The court found that United Shore implicitly waived privilege to the reports when it disclosed its conclusions.

Protecting Incident Response Under Privilege

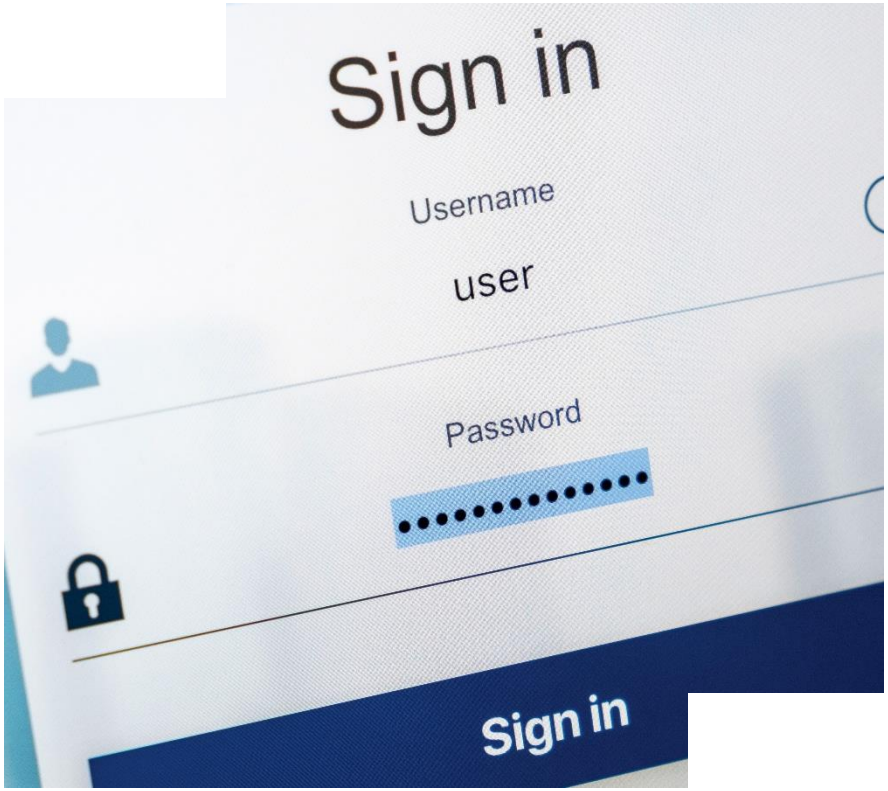
Best practices

1. Consider adding outside counsel to **ALL** internal and external correspondence, including phone calls, e-mail and text messages
2. Consider directing all internal and external correspondence to outside counsel
3. Consider marking attorney correspondence with “attorney–client privilege/confidential”
4. Consider marking reports generated in anticipation of litigation with “work product” on each page

Protecting Incident Response Under Privilege

Best practices

5. You may want outside counsel to retain and direct the work of the cybersecurity consultants
6. You may want to exercise caution when sharing information about Incident Response with third parties
7. Consider limiting employees with access to privileged information



Thank you!

Kroll | A Division of DUFF & PHELPS

Snell & Wilmer

For more information about our global locations and services, please visit:
www.kroll.com
www.swlaw.com

Contacts

Jonathan Fairtlough
Managing Director
Cyber Risk
jfairtlough@kroll.com

James P. Melendres
Partner
Chair, Cybersecurity, Data Protection, and Privacy Practice
jmelendres@swlaw.com