Exploring Cyber Liability Concerns and Options

Facilitated by:
Yvonne Castillo
Victor O. Schinnerer & Company, Inc.

Presented by:
Jennifer Coughlin, Mullen Coughlin, and
Bill Hardin, Charles River Associates

December 13, 2018

Exploring Cyber Liability Concerns and Options

Credits earned on completion of this course will be reported to AIA CES for AIA members. Certificates of Completion for both AIA members and non-AIA members are available upon request.

This course is registered with AIA CES for continuing professional education. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing, or dealing in any material or product.

Questions related to specific materials, methods, and services will be addressed at the conclusion of this presentation.

AIA CES Details

For AIA/CES purposes the provider of this program is:
Victor O. Schinnerer & Company, Inc.
Provider Number: K048

Exploring Cyber Liability Concerns and Options
Course Number: VOS 604-DE

The speakers for this program are:

Jennifer Coughlin
Mullen Coughlin
and
Bill Hardin

Yvonne Castillo
Director, Risk Management
Victor O. Schinnerer & Co, Inc.
Chevy Chase, Maryland

December 13, 2018

Disclaimer

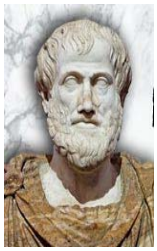
MULLEN COUGHLIN LLC

CRA Charles River Associates

The material presented in this presentation is not intended to provide legal or other expert advice as to any of the subjects mentioned, but rather is presented for general information only. You should consult knowledgeable legal counsel, forensic experts, or other knowledgeable experts as to any legal or technical information.

Neutral

Why Do We Do It? – The Art of Rhetoric



Ethos

Pathos

Logos

"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

Game Theory in Practice

Extortion Threat Landscape

ENGAGEMENT

AUTOMATION

Extortion Request 1

@Hello! I'm a member of an international hacker group.

As you could probably have guessed, your account [email address] was hacked, because I sent message you from your account.

Now I have access to all your accounts! For example, your password for [insert service/password]

Within a period from July 30, 2018 to October 9, 2018, you were infected by the virus we've created, through an adult website you've visited. Moreover, we've gotten full damps [sic] of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know.. But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched! I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $800 to our Bitcoin wallet: 1GdegtNpYcvoCPsMmyiSkZARDdAmYuXGXU

If you don't know about Bitcoin please input in Google "buy BTC". It's really easy. I guarantee that after that, we'll erase all your "data" :)

A time will start once you read this message. You have 48 hours to pay the above-mentioned amount. Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection. You should always think about your security. We hope this case will teach you to keep secrets.

Extortion Request 2

Dear John,

We gained access to some things that we probably shouldn't have had access to. After looking through these files and information we found something that stood out to us. Pricing information, employee data, customer lists, etc..

Like you, we are a for-profit group. Due to security reasons we are only able to receive our payment in bitcoin. If you are interested in keeping this information private, please send 70 bitcoins to the bitcoin address listed at the very bottom of this email.

We advise you to keep this confidential.

Bitcoin Address:
1P4STNLNAOGNrLRFCyER2vfQVjKRMG7ihGDoy8

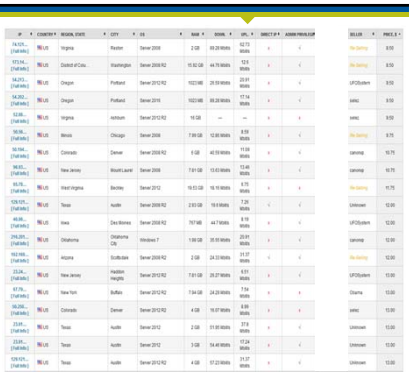
Two days. noon pacific time.

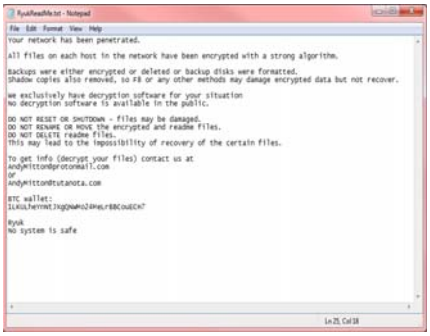
Automation – We Call It

BTCWare BitPaymer vCrypt Merry I love you Bruce Locky Stampado Zelta

Lockout SAMSAM Matrix Cerberos Cry9 Serpent Troldesh Jigsaw

JeepersCrypt CryptoMix Petya Erebus WANNACRY NotPetya Bad Rabbit Reveton Mole66 RYUK CryptON





Business Interruption

Systems Impacted

Communications- Internal/External

System Upgrades

Payroll

Client Requests

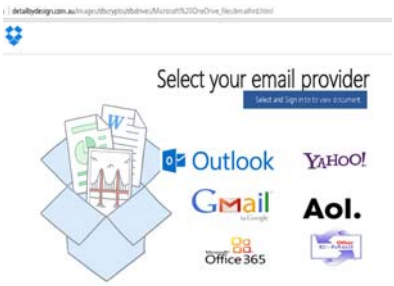
Business Competitors

Example – Phishing Email Subjects

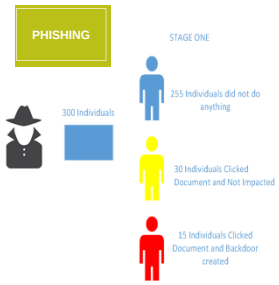
- Urgent Action Required
- Storage Space Exceeded
- Security Alert
- Password Expiring
- UPS Deliver Notice
- Job Satisfaction Survey
- DocuSign document T247218
- Bill Shared a File With You
- USPS: Failed Delivery Notice
- Unusual Sign Activity-Verify Your Identity
- Microsoft: Your account will be deactivated

Victor O. Schinnerer & Company, Inc. 15

Phishing Sites



Victor O. Schinnerer & Company, Inc. 16



Victor O. Schinnerer & Company, Inc.

Business Email Compromise: Attack Methodology, Information and Theft

Phishing / Spam Emails	Email Spoofing and Impersonation	Unauthorized Inbox Rules / Forwarding	Malware
Malicious Macros / PDFs	Contact Harvesting	PCI	PHI
PII	Passwords Stored in Email	Other Platforms Exposed	Compromised VPN Credentials
Wire / Bank Fraud	Direct Deposit / Payroll Fraud	Tax Return Fraud	Theft of Intellectual Property

Victor O. Schinnerer & Company, Inc.

Victor O. Schinnerer & Company, Inc.

SECURITY MATTERS

Victor O. Schinnerer & Company, Inc.

Ever Changing Definitions (U.S.)

- **Personally identifiable information (PII)** - i.e., Social Security number, driver's license number, state ID, financial information, credit card information, online/financial account username and password, medical information, health insurance information, and email address and password
- **Protected health information (PHI)** - Information created or received by a covered entity or business associate **relating to the past, present or future physical or mental health** or condition of an individual; the provision of healthcare to an individual; or the past, present, or future **payment for** the provision of health care to an individual, that identifies or can be used to identify the individual
- **Payment card industry information (PCI**) - Cardholder data
- **Contracts**

Victor O. Schinnerer & Company, Inc.

State Regulatory Exposures

- **50 states** (plus Puerto Rico, Washington D.C., Virgin Islands, Guam) require notice to residents after unauthorized access to personally identifiable information
- Require companies to **notify resident consumers** of security breaches of unencrypted computerized personal information (includes health information in some states)
- Many require notification of **state attorney general**, state consumer protection agencies, and credit monitoring agencies
- Notice due "**without unreasonable delay**", but some strict states (30/45/90 days)
- Some states are requesting an **Assurance of Voluntary Compliance**
- Some states allow **private right** of action for violations

Victor O. Schinnerer & Company, Inc.

States That Updated Regulations in 2017

California
- Clarified breach of encrypted data **with encryption key** requires notice

Illinois
- **Adds data to definition of PI**: medical information, health insurance information, unique biometric, username/email address and password/security question and answer
- Clarified breach of **encryption key** requires notice
- **Added Regulator Notice**:
  - HIPAA Covered Entities must notify IL AG within 5 business days of notifying HHS
  - State agencies must notify AG when 250 or more affected

Virginia
- Requires **notification to AG of employer FEIN** if breach includes TIN and income tax withheld of employees or if breach occurs at payroll provider

New Mexico
- 48th State to enact
- Notice within 45 days after discovery of breach of computerized data
- Notice Attorney General and consumer reporting agencies if more than 1,000 New Mexico residents are notified.
- Defines PII as name in combination with Social Security Number, Driver's License Number, Government ID Numbers, Financial Account numbers, Biometrics Data

Tennessee
- Clarified **encryption safe harbor** in April: breach of encrypted data (without loss of encryption key) does NOT require notice.

Victor O. Schinnerer & Company, Inc.

States That Updated Regulations in 2018

Maryland

- Effective January 1, 2018
- **Expands definition of PI** to include: passport number, state ID, health information, health insurance policy number, biometric data, and username and password
- Requires notice within **45 days** of discovery

Oregon

- Effective June 2, 2018
- Expands definition of PII to include any information, along with a financial account number, which would permit access to a financial account
- **Notice within 45 days** of discovery of a breach
- Does not allow consumer reporting agencies to charge fees to place or lift a security freeze

Delaware

- Effective April 14, 2018
- **Expands definition of PI** to include: biometric data, medical information, passport numbers, routing numbers, TINs, and usernames
- Requires one year of **credit monitoring** for breaches involving SSNs
- **Notice to Attorney General** if more than 500 Delaware residents are affected
- Notice within **60 days** after discover of a breach

Alabama

- Effective **June 1, 2018**
- **Notice within 45 days** after discovery of breach of computerized data
- Notice to Attorney General and consumer reporting agencies if more than **1,000 Alabama** residents are notified.
- Defines PII as name in combination with **Social Security Number/TIN, State Issued ID/Passport/Military Identification number, Financial Account numbers, Medical Information, Health Insurance Information, Username/Email address with Password**

States That Updated Regulations in 2018

South Dakota

- Effective **July 1, 2018**
- **Notice within 60 days** after discovery of breach of computerized data
- Notice to Attorney General if more than **250 South Dakota residents** are notified.
- **Notice to Consumer Reporting Agencies** if one or more SD residents are notified
- Defines PII as name in combination with **Social Security Number, Driver's License Number, Employee ID Numbers with Biometric Data, Financial Account numbers, Health Information, Username/Email address with Password**

Colorado

- Effective September 1, 2018
- Requires implementation of **"reasonable security procedures and practices"** to protect personal identifying information
- Expands definition of PII to include **student, military, or passport number, medical information, health insurance identification number, biometric data, username/password**
- **Notice within 30 days** of discovery of a breach
- Notice to Attorney General if **500 or more Colorado** residents are impacted
- Creates obligations for Colorado governmental entities

Arizona

- Effective July 16, 2018
- **Notice within 45 days** after discovery of a breach
- **Expands definition of PI** to include: biometric data, medical information, health insurance information, passport numbers, routing numbers, TINs, and usernames
- **Notice to Attorney General** and consumer reporting agencies if more than 1,000 Arizona residents are affected
- Changes **substitute notice** requirements to include notice to AG regarding why substitute notice is necessary and **website posting for 45 days**
- Increases civil penalties for knowing violation of the statute to **$500,000 per breach**

South Carolina

- Effective January 1, 2019 – **Department of Insurance Data Security Bill**
- Requires insurers, agents and other entities licensed by Department of Insurance to **develop and maintain written information security program** based on risk assessment
- Requires notification to Dept. of Ins. **within 72 hours** of a cybersecurity event involving a SC-domiciled licensee or if more than 250 SC residents are impacted
- Notification to individuals required without undue delay

States That Updated Regulations in 2018

Virginia

- Effective **July 1, 2018**
- **Tax Return Preparers** must notify the Department of Taxation of a compromise of Virginia residents' "return information" Defines return information to include "taxpayer's identity" and income, payments deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, assessments or tax payments

Connecticut

- Effective **October 1, 2018**
- Eliminates fees for placing or lifting a security freeze with the consumer reporting agencies
- **Requires 24 months of credit monitoring services when an individuals' SSN was exposed in a breach**

Vermont

- Effective January 1, 2019
- Data brokers must **register annually** and provide information about their **data collection activities** and opt out policies
- Data brokers must **adopt an information security program** which include administrative, technical and physical safeguards
- **Defines** data broker to be a business that "knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship"

States That Updated Regulations in 2018

Louisiana

- Effective August 1, 2018
- Expands definition of PI to include: state ID number, passport, and biometric data.
- Requires the implementation and maintenance of reasonable security procedures and practices.
- Requires the destruction of PII that is no longer to be retained.
- Requires notice within 60 days of discovery.
- Permits substitute notice where notification would exceed $100,000 or notifying more than 100,000 affected residents.
- Notice not required if there is no reasonable likelihood of harm. Determination must be documented.
- Violation of the law constitutes an unfair act or practice.

Hawaii, Iowa, Illinois, Kentucky, Michigan, Nebraska, New Hampshire, Washington

- **Eliminated fees for consumers** for placing or lifting a security freeze with the consumer reporting agencies

Bills Pending in 15 states

States With Changing Regulations 2020

California

- California lawmakers passed the most aggressive privacy law in the United States, the California Consumer Privacy Act of 2018
- Takes effect on January 1, 2020
- The Act will apply to for-profit businesses that collect and control California residents' personal information, do business in the State of California, and: (a) have annual gross revenues in excess of $25 million; *or* (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; *or* (c) derive 50 percent or more of their annual revenues from selling California residents' personal information.
- Broadens definition of "personal information", including the following: consumer's personal identifiers, geolocation, biometric data, internet browsing history, psychometric data, and inferences a company might make about the consumer
- Major Provisions:
  - Provides consumers with the right to be informed about the kinds of personal data companies have collected and why.
  - Consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a "readily useable format" that enables its transfer to third parties without hindrance.
- The Act can be enforced by the California Attorney General, subject to a thirty-day cure period. The civil penalty for intentional violations of the Act is up to $7,500 per violation.
- The Act also provides a private right of action that allows consumers to seek, either individually or as a class, statutory or actual damages and injunctive and other relief.

HIPAA: To Whom Does it Apply?

- Covered Entities —
  - Health care provider — **i.e., doctor, nursing home, pharmacy, hospital**
  - Health plan — **i.e., health insurance companies, HMOs, self-funded company health plans, government programs that pay for health care**
  - Health care clearinghouse — **i.e., health information processing company**
- Business Associates —
  - Entity that uses or discloses PHI and performs certain functions on behalf of a Covered Entity
    - **i.e., collections, claims processing, billing, attorney**

HIPAA: What Is A Breach?

- A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information
- An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
  1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  2. The unauthorized person who used the protected health information or to whom the disclosure was made;
  3. Whether the protected health information was actually acquired or viewed; and
  4. The extent to which the risk to the protected health information has been mitigated

Victor O. Schinnerer & Company, Inc.

HIPAA: Breach Notification Rule

- Deadline for breach reporting begins running from **"discovery"**
- Individuals — without unreasonable delay and in no case later than **60 business** days from discovery
  - Written and /or substitute
- HHS — without unreasonable delay and in no case later than 60 calendar days from discovery (over 500 affected), or no later than 60 calendar days following the year in which the breach occurred (less than 500 affected)
- Media — without unreasonable delay and in no case later than 60 calendar days following discovery (over 500 in one state or jurisdiction)

Victor O. Schinnerer & Company, Inc.

HIPAA: Privacy Rule

- Designate a Privacy Officer
- Develop and Implement HIPAA Policies and Procedures
- Provide and Document HIPAA training for staff
- Minimum Necessary – Secure patient records containing PHI so that they are not readily available to those who do not need them
- Business Associate Agreements
- Patient rights regarding access and sharing of their own health information

Victor O. Schinnerer & Company, Inc.

HIPAA: Security Rule

- *Implement safeguards to protect the confidentiality, integrity, and availability of electronic protected health information*
- Gets into specifics regarding data use and management
  - Risk Assessment and Risk Management Plan
  - Encryption, Passwords, Email procedures
  - Security Incident monitoring and procedures
  - Back-up and data destruction
  - Etc.

HIPAA: Enforcement Rule

- Violation Category
  - (A) Did Not Know ..... $100–$50,000
  - (B) Reasonable Cause ..... $1,000–$50,000
  - (C) Willful Neglect
    - i. Corrected .....$10,000–$50,000
    - ii. Not Corrected $50,000
- $1.5 million per year cap per violation type.

HIPAA: OCR Investigations

- OCR will likely investigate any breach involving **over 500** affected individuals
- OCR will request information relating to compliance of the Privacy Rule, Security Rule, and Breach Notification Rule at the time of breach reporting, and in subsequent investigation
- Responses to a request for information are due within twenty (20) to thirty (30) days of the date of OCR's request
- The length of an investigation may vary — **can be years**
- OCR will attempt to resolve the investigation with the covered entity by obtaining:
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement.
- If an OCR investigation results in a finding of non-compliance of HIPAA, HHS may initiate a formal enforcement action that may result in the imposition of civil money penalties, or take other actions consistent with OCR's jurisdiction, including the referral of the complaint to the Department of Justice for investigation
- To prepare for OCR investigation some covered entities are taking steps to achieve voluntary compliance to mitigate potential fines that may result from a breach

Payment Card Industry (PCI)

- Payment Card Industry Security Standards Council (Visa, Mastercard, AmEx, Discover, JCB International)
- Requires merchants and service providers to abide by certain protocols to protect customers' credit card information
- Imposes "assessments" and "fines" on offending merchants and service providers (can be millions)
- Violations of PCI DSS have multiple consequences
- Impact on standard of care — industry investigations, outside lawsuits
- Small minority of states have incorporated PCI-DSS requirements into data protection laws
- **Privileged forensics vs PFI**

Victor O. Schinnerer & Company, Inc.

Overview of the EU General Data Protection Regulation (GDPR)

- Went into effect on May 25, 2018 and is binding on all EU Member States. The UK agreed to enforce GDPR despite Brexit.
- The EU considers the protection of natural persons in relation to the processing of their personal data as a **fundamental right**. GDPR also includes a **broad definition of personal data** – any information relating to an identified or identifiable natural person.
- Applies to processing that occurs in the EU. Also applies to processing of personal data of data subjects in the EU (even when processing occurs outside of the EU) when the processing relates to: (1) offering of goods/services to EU citizens or (2) monitoring behavior that occurs in EU.
- Sets forth requirements for – among other things – technical and organizational security measures, record keeping, designation of representatives/DPOs, and international data transfer.

Victor O. Schinnerer & Company, Inc.

Overview of the EU General Data Protection Regulation (GDPR)

- Provides for individual rights (to be informed, access, rectify, erasure, restrict processing, data portability, object, and rights related to automated decision making/profiling).
- Breach Notification
- Requires notice to the Supervisory Authority competent within 72 hours of a breach, unless the breach is unlikely to result in risk to the rights and freedoms of natural persons.
- Requires notice to data subjects without undue delay when the breach is likely to result in high risk to the rights and freedoms of natural persons.
- Maintains a tiered approach to fines, which can be up to 20 million euros or 4% of worldwide annual turnover from the preceding year.

Victor O. Schinnerer & Company, Inc.

Anatomy of a Breach Response

BREACH DISCOVERY

EXPERTS
- Breach coach
- Forensics
- Public relations

INVESTIGATION - internal/forensic/criminal
- How did it happen?
- When did it happen?
- Is it still happening?
- Who did it happen to?
- What was accessed/acquired? (What wasn't?)

NOTICE OBLIGATIONS
- State
- Federal
- Other (i.e. PCI)
- Deadlines – Can be 48 hours

NOTIFICATION

PROCESS
- Written
- Electronic
- Substitute
- To Media

VENDORS
- Printing, Mailing and Call Center
- Credit Monitoring

INQUIRIES
- State Regulators (i.e. AG, PD)
- Federal Regulators (i.e. OCR)
- Federal Agencies (i.e. SEC, FTC)
- Consumer reporting agencies
- Potential Plaintiffs

LITIGATION
- Government Entities
- Class Action
- Indemnification

Best Practices Post-Incident

- **Ensure experience** on Response Team
  - Post data incident is not the time to learn the ins and outs of incident response
  - Establish **Incident Response Team** of decision-makers (if not established already) as things move too fast for typical bureaucracy
- Use Counsel to Establish **Privilege**
  - Counsel directs forensics, notice drafting, and other vendors so that, in the event of litigation or regulatory investigation, all documents and communications are not discoverable
  - Guard Attorney-Client Privilege: **do not** share forensic reports, legal analysis and drafts with clients or third parties if not absolutely necessary
- Do not **use terms "Breach" or "PII" or "PHI" lightly** — these are statutorily defined legal terms the use and admission of which have consequences

Best Practices Post-Incident

- Do **not rush** to go public
  - Tremendous desire to go public fast, but an inability to answer questions that will inevitably follow can be devastating
  - **If you notice goes out 4 hours after discovery, there will be people who charge you with delay, so "delay" is unavoidable**
- **Prepare for litigation** and regulatory investigation — Preserve all relevant documents
- Conduct **risk assessment** and implement **data security improvements** prior to being asked by a regulator

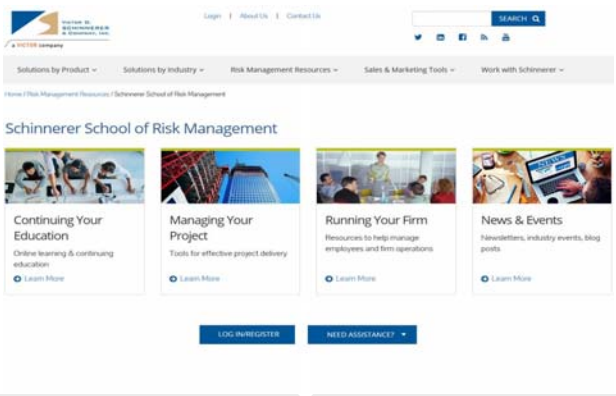
Best Practices Pre-Incident

- **Empower** the organization's First Responders
- **Talk** to your IT Security folks. Gain an appreciation of the many challenges and risk landscape
  - Not many Firms can say: how many records they have; what type of data is being collected, stored, shared, protected; where does all this data reside; when is it purged?
- **Assess and test the organization's** staff and operations
- Prepare and **test your incident response plan**
- **Document** your due care measures (training and enforcement) being taken
- **Insure** yourself
- Repeat

Thank You

Jennifer Coughlin
jcoughlin@mullen.law
631-987-7488 Cell
267-930-4774 Office
www.mullen.law

Bill Hardin
bhardin@crai.com
773-415-3076 Cell
312-619-3309 Office



Exploring Cyber Liability Concerns and Options

This concludes a course approved by:

The American Institute of Architects Continuing Education Systems

Victor O. Schinnerer & Company, Inc.

Contact Information:

Andrea Tyler

Andrea F. Tyler@Schinnerer.com