

EXCLUSIVELY FOR



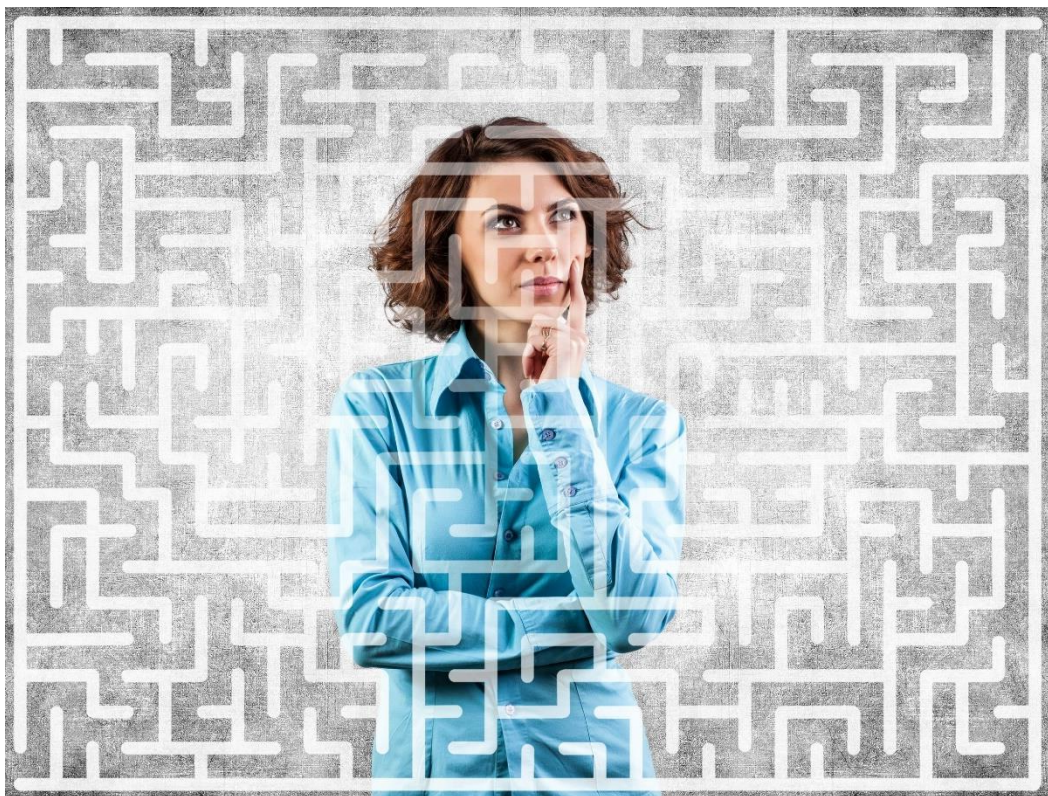
What the FBI Didn't Tell You

The Non-technical
CEO's Guide
to Ransomware
& Email Scams



This webinar should not be considered legal advice.

We want you to move from WONDERING to CONFIDENT



- Chair, Privacy and Data Security practice group
- Represents companies in various industries from startups to Fortune 100
- Pre-breach counselor
- Breach response coach
- Distinguished Fellow – Ponemon Institute
- Professor of Information Security Policy and Law
- Recognized by Chambers USA since 2015 for complex commercial litigation
- J.D. from Fordham, Ph.D. from NYU, B.A. from University of Rochester





Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

New York Law Journal

AN ALM PUBLICATION
MONDAY, AUGUST 28, 2017
VOLUME 258—NO. 40
Outside Counsel
Expert Analysis

Grace Period Expires for Cybersecurity Regulations in NY: What Comes Next?

The day has finally arrived for the financial services industry in New York. The new cybersecurity regulations issued by the New York State Department of Financial Services are officially in force, after a 180-day grace period that



global reach that DFS attached a two-year phase-in period to the Third Party Service Provider Security Policy requirement. Second, by choosing the regulatory process to implement Part 500, New York has doubled down on the trend in cybersecurity regulation to infer broad regulatory authority from consumer protection provisions.

New York Law Journal

AN ALM PUBLICATION
MONDAY, OCTOBER 23, 2016
VOLUME 257—NO. 43
Outside Counsel
Expert Analysis

New Regulations Add to Complexity Of Cybersecurity Compliance

On Sept. 13, 2016, the New York State Department of Financial Services (DFS) published draft regulations addressing cybersecurity in the financial services industry. The regulations are sweeping in scope and reach, covering all financial institutions, such as banks and credit unions, and all financial services providers, such as fintech companies, and all financial services providers, such as fintech companies, and all financial services providers, such as fintech companies.



There, however, lies the rub. Do the new rules apply to the bank's entire operations, or only to the most complex portion of its business? Do the exceptions in the regulations (based on size or on whether the bank is a public company) apply to the bank as a whole, or only to the DFS-regulated activities only? And does such a distinction even make a difference, because it is unlikely that a bank has dedicated systems and security measures for its DFS-regulated operations only? The regulations provide no guidance on these issues, and the trend in cybersecurity regulation is for greater rather than

New York Law Journal

CORPORATE UPDATE
AN ALM PUBLICATION
THURSDAY, MARCH 29, 2016
VOLUME 255—NO. 10
FINANCIAL SERVICES
Expert Analysis

NY DFS Issues Sweeping FAQs Affecting Scope of Regulations

The cybersecurity regulations from the New York State Department of Financial Services (DFS) that went into effect on March 1, 2017 have had wide-reaching effects in the financial services industry and beyond. Their sweeping scope—applying to any person or entity licensed or otherwise operating under an authorization under the New York Banking, Insurance, or



Open questions remained for other entities, however, especially federally chartered banks that function as "excepted mortgage servicers" in New York and certain health care entities, such as Health Maintenance Organizations (HMOs) and Continuing Care Retirement Communities (CCRCs). DFS's primary justification for regulatory guidance in relation to Part 500 has been its "broad" language—available to

New York Law Journal

AN ALM PUBLICATION
WEDNESDAY, SEPTEMBER 13, 2017
VOLUME 258—NO. 37
Outside Counsel
Expert Analysis

The Equifax Breach: Why This One Is Different

On Sept. 7, 2017, the credit reporting agency Equifax reported a data breach affecting approximately 143 million U.S. consumers. Among the personally identifiable information (PII) that was compromised was name, date of birth, address, and Social Security



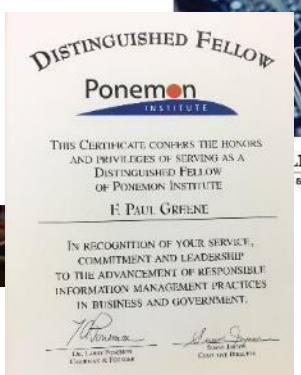
the effect on the organizations that employ or serve these individuals is more indirect, and nuanced. At a minimum, the compromise of such a large amount of highly sensitive PII for such a large portion of the U.S. adult population should cause organizations large and small to consider whether this breach has increased their own risk in any material fashion. Against this backdrop, questions abound, but answers are not always clear.



Financial institutions and fintech companies, but not consumer protection provisions.



Are you ready for DFS's new cybersecurity regulations?



Exclusive event to get you on track for NYS DFS's cybersecurity regulations

Tuesday, May 16, 2017

Pathway to Compliance: What does NY DFS 23 N.Y.C.R.R. Part 500 really mean to your organization?



Rochester Business Journal (RBJ)

NOVEMBER 11, 2014

New cybersecurity regulations need clarification



The state has placed a great deal of emphasis on the need for cybersecurity regulations, but none of the language surrounding the rules remains unclear, says Paul Greene, partner at Harter Secrest & Emery LLP.

Proposed rules limit how long lenders can wait to report acts of cybercrime. By SHEILA LEVADAS. Though still in draft form and likely to spark further guidance from the state once the comment period ends, the regulations need clarification, some legal experts say. Issued in September by the state Department of Financial Services, the proposed cybersecurity regulations require financial service entities under the department's supervision to establish programs and policies that aim to detect and prevent, such as network scans and data backups, from giving unauthorized access to their information systems. Other aspects of the rules require entities under the department's supervision to conduct risk assessments on their information systems at least once a year.

Reprinted with permission of the Rochester Business Journal.



Mike Semel

- 40-year IT business owner/manager
- 16-year certified HIPAA Professional
- EMT/ER Tech/FD Rescue Captain/IndyCar Safety Team
- Hospital Chief Information Officer (CIO)
- School District Chief Information Officer (CIO)
- Cloud Backup Service Chief Operating Officer
- Member, FBI Infragard
- Chair, CompTIA Security Community (retired)



Mike Semel

President
Chief Compliance Officer
SEMEL Consulting



Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY



Speaking, Writing



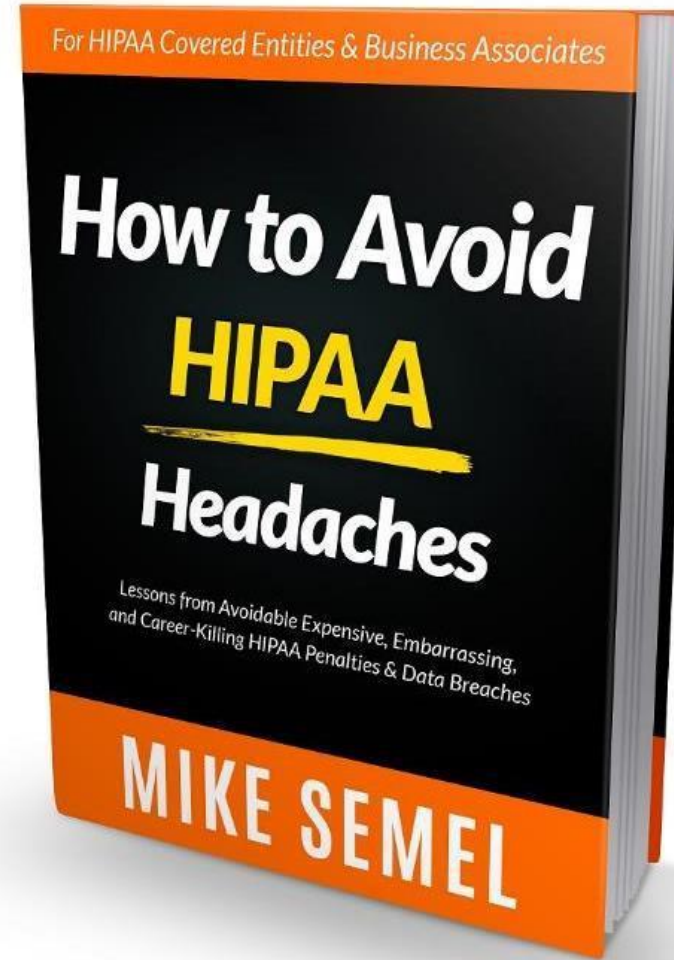
Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

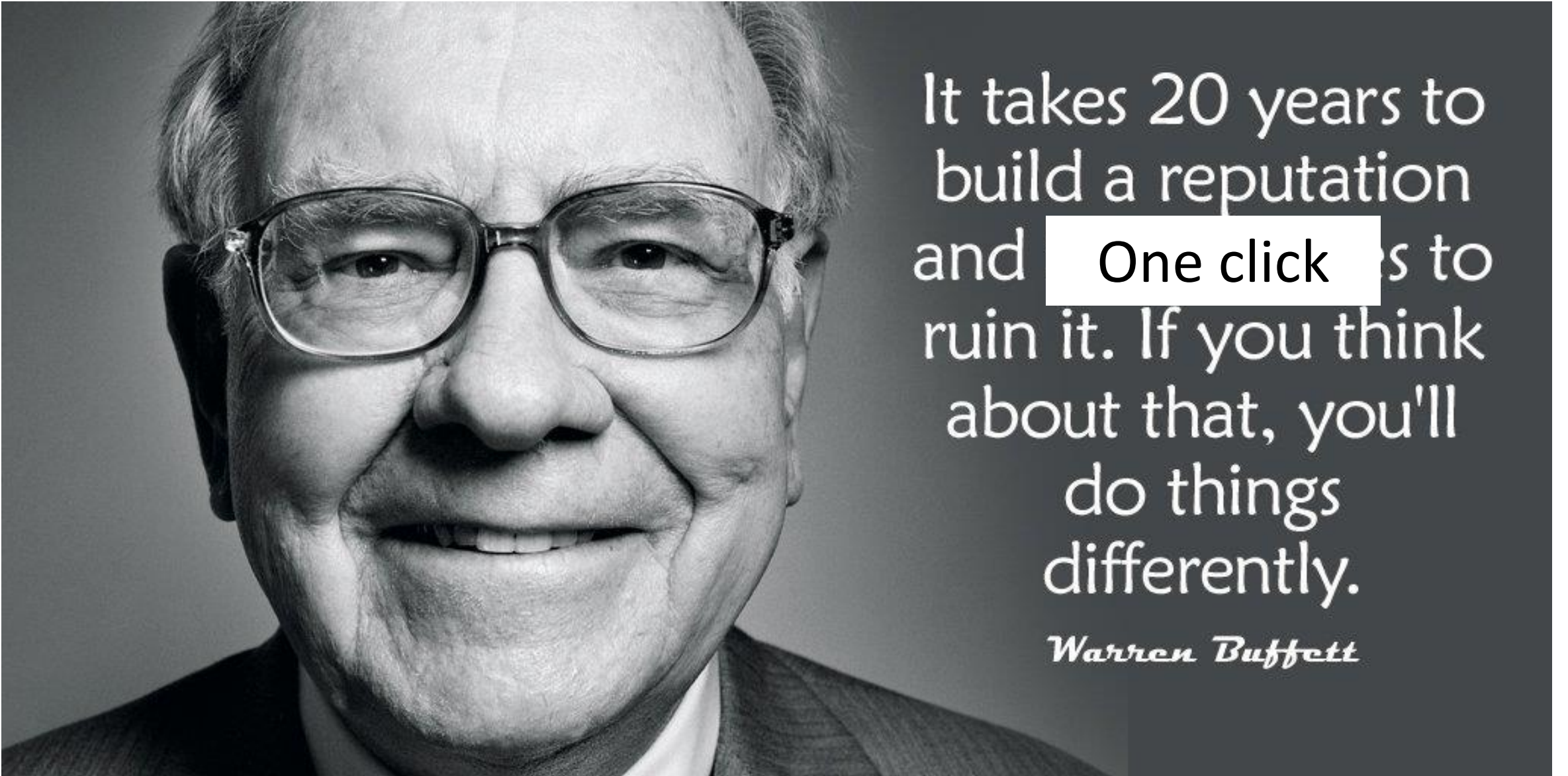
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY



Amazon Best-Seller



Cyber Security Is a BUSINESS problem With a TECHNICAL solution



It takes 20 years to
build a reputation
and **One click** is to
ruin it. If you think
about that, you'll
do things
differently.

Warren Buffett

2019 FBI Cyber Warnings



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



September 10, 2019 Alert Number **I-091019-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS EMAIL COMPROMISE THE \$26 BILLION SCAM



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



October 02, 2019 Alert Number **I-100219-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS

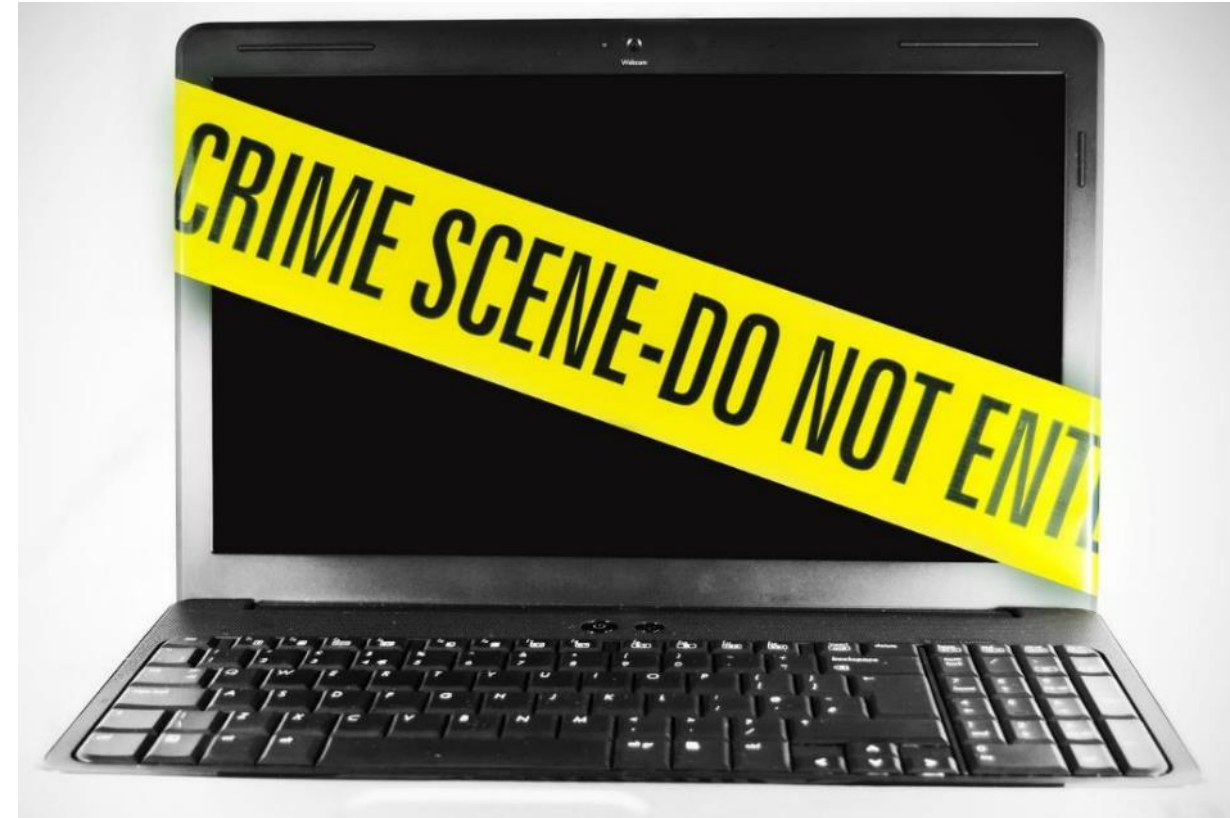
Business Email Compromise

Email 'from 'the boss''

- Funds Transfer
- Payroll Information
- Gift Card Purchase

Email 'from an employee'

- Direct Deposit Redirection



Ransomware

- A type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.
- Typically spreads through phishing emails or by unknowingly visiting an infected website.



Backups Help Recover From Ransomware, but...

- Backups are no good unless you can recover both reliably and quickly.
- Some victims of ransomware have had backups but still have had to pay the ransom because the backup schedule did not perform backups with enough granularity, or they were not backing up the data they thought they were backing up.



High-Impact Ransomware Deletes Backups



High-Impact Ransomware Deletes Backups

MAR 23, 2018

New Strain of Ransomware Deletes Backup Data

**It's all fun and
games until
ransomware
deletes the
shadow copies**

Ransomware Growth

2019 - \$ 2 trillion (Juniper)

2021 - \$ 6 trillion (Forbes)

Security Is More Important Than Ever

Beazley breach insights - October 2019



Small Businesses = Big Ransomware Targets

2018

70 percent of ransomware attacks targeted small businesses

Average ransom demand of \$116,000

Beazley Breach Response Services.

Cost of Ransomware

Advisen

Costs of business downtime from ransomware 23 times higher than ransom demand: report

- 64% - loss of business productivity
- 34% - lost data or devices
- 45% - business-threatening downtime
- 18% - reputational damage

Wood Ranch Medical Announces Permanent Closure Due to Ransomware Attack

Cost of Ransomware

\$ 116,000

x 23 =

\$ 2.668 million

Average Ransom – Beazley Insurance Report

Downtime = 23 x Ransom – Advisen Report

Will Your Cyber Liability Insurance Pay Off?



Insurer Seeks Breach Settlement Repayment

Alleges Client Failed to Follow 'Minimum Practices'

Columbia Casualty alleges that Cottage Health's application for coverage under the Columbia policy "contained misrepresentations and/or omissions of material fact that were made negligently or with intent to deceive concerning Cottage's data breach risk controls," according to the insurer's lawsuit.

Business Email Compromise Impact

- Financial Losses
- Pain to Individuals You Serve
- Pain to Workforce Members
- Reputational



Business Email Compromise Legal Impact

- Lawsuits
- Regulations



Regulations

- HIPAA
- NYS Data Breach Law
- NYS SHIELD Act



HIPAA - Ransomware is a Breach

HHS Office for Civil Rights in Action



FACT SHEET: Ransomware and HIPAA

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

HIPAA Breach Notification Rule Exceptions

- ...**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:**
 - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - The unauthorized person who used the protected health information or to whom the disclosure was made;
 - Whether the protected health information was actually acquired or viewed; and
 - The extent to which the risk to the protected health information has been mitigated.

THESE ARE NARROW EXCEPTIONS - NOT BIG LOOPHOLES

NY State Data Breach Law

- **Protects the following data if acquired without authorization**
 - Social Security Number
 - Driver's License or non-driver ID
 - Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.



IMPORTANCE TO ARCS:

INDIVIDUALS – SS# AND BANK ACCOUNT INFO
HR RECORDS OF APPLICANTS, CURRENT EMPLOYEES, FORMER EMPLOYEES; CURRENT AND PAST CONTRACTORS; ACCIDENT REPORTS

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY



NY SHIELD Act - Ransomware is a Breach

- **Changes breach to include 'access' to data instead of just 'acquiring' data**
- **Requires reasonable data protection**
- **Failure considered an unfair business practice**



NY SHIELD Act - Ransomware?

Factors for determining if a breach has occurred:

- ***“indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.”***



NY SHIELD Act - Other Compliance Laws

- **Businesses that are already regulated by and comply with data breach notice requirements** HIPAA, NY DFS Reg 500, Gramm-Leach-Bliley Act, **are not required to further notify affected New York residents**
- **Still required to notify the New York attorney general, the New York State Department of State Division of Consumer Protection, and the New York State Division of the State Police.**



NY SHIELD Act - Other Compliance Laws

- **SHIELD does not apply to any person or business subject to and compliant with the security requirements of GLBA, HIPAA, Part 500, or “any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government”**
- **Section §899-bb is silent as to how an entity can prove that it is compliant** with any of these regulatory schemes.
- **Because compliance is measured at a point in time, it is possible** under §899-bb for a bank subject to GLBA or a hospital subject to HIPAA **to fall out of compliance with their primary regulator, and therefore become ineligible for the “compliant regulated entity” caveat built into §899-bb.**



New York Law Journal

F. Paul Greene, Attorney, Harter-Secret

NY SHIELD Act - Reasonable Safeguards

Businesses must **develop, implement and maintain** reasonable safeguards to protect the **security, confidentiality and integrity** of the private information.



NY SHIELD Act - Administrative, Technical, Physical Security Examples defined in law

- Risk assessments
- Employee training
- Selecting vendors capable of maintaining appropriate safeguards
- Implementing contractual obligations for those vendors
- Disposal of private information within a reasonable time period



NY SHIELD Act - Penalties

- **No private right of action (but...)**
- **Class action litigation is not available.**
- **Attorney general may obtain civil penalties.**
- **For data breach notification violations that are *not* reckless or knowing, the court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses.**
- **For knowing and reckless violations, the court may impose penalties of the greater of \$5000 dollars or up to \$20 per instance with a cap of \$250,000.**
- **For reasonable safeguard requirement violations, the court may impose penalties of not more than \$5,000 per violation.**



NY SHIELD Act - Basis for Litigation

“...enterprising litigants are certain to refer to (the SHIELD Act’s) substantive security requirements as a new floor in New York, at least when alleging negligence in relation to a data breach.”



New York Law Journal

F. Paul Greene, Attorney, Harter-Secret

Insurance



Incident Response

- Coach Services
- Credit Monitoring
- Forensics
- Legal
- Notification
- Public Relations
- Rewards



First Party Coverages

- Business Interruption
- Contingent Business Interruption
- Extortion
- Digital Data Recovery
- Financial Fraud
- Telecom Fraud

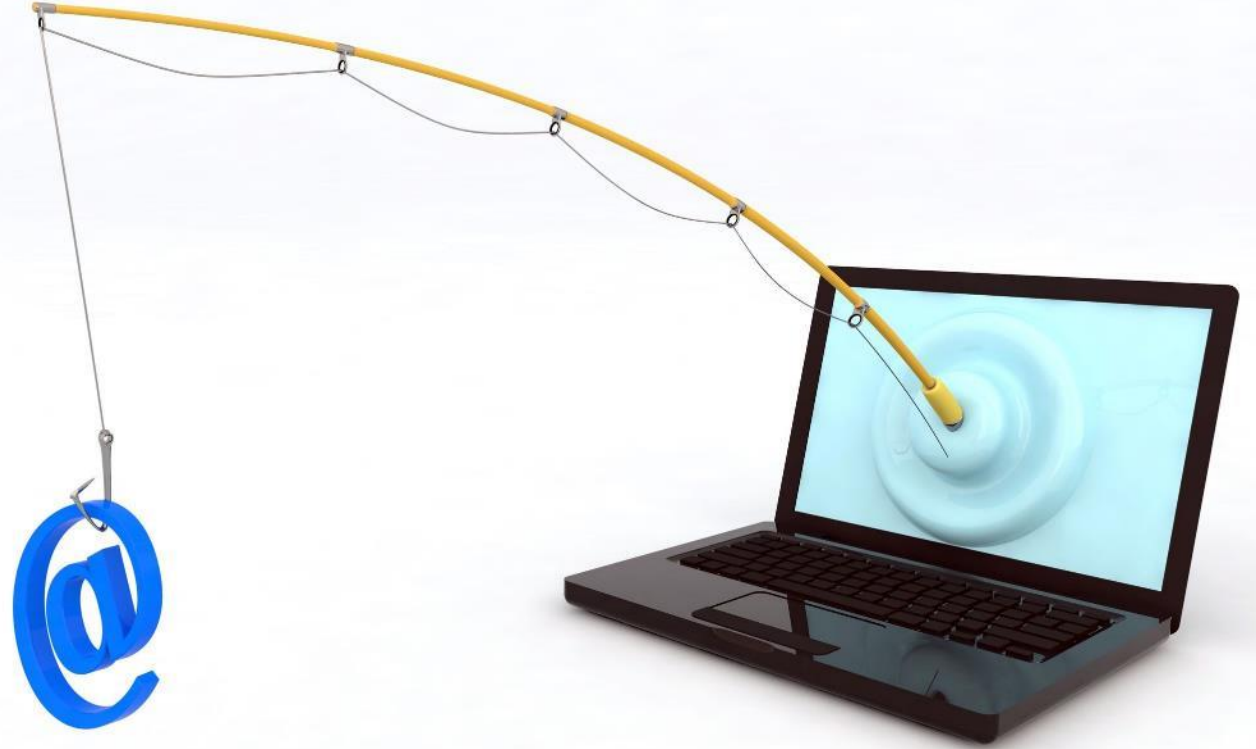


Third Party Coverages

- Media Liability
- Network Liability
- Payment Card Loss
- Privacy Liability
- Regulatory Risk
- Technology E&O

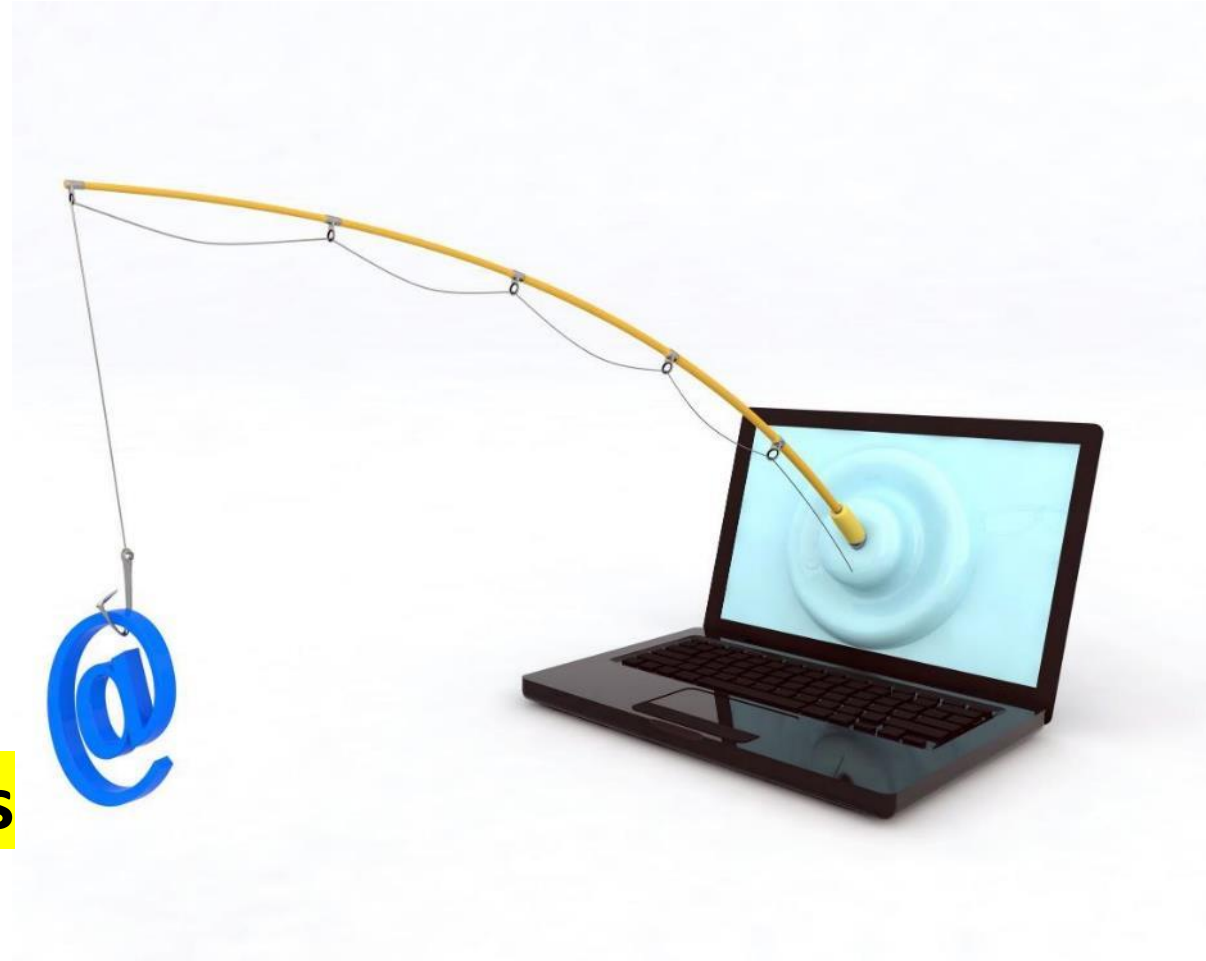
Strategies to Protect Against Business E-Mail Compromise

- **Train Users to Avoid Phishing Scams**
- **E-mail Protection System**
- **Tag [External] email**
- **Require personal validation via a call or face-to-face**
- Preparation - Policies, Procedures, Evidence
- Insurance



Strategies to Protect Against Ransomware

- **Train & Test Users to Avoid Phishing Scams**
- **E-mail Protection System**
- **Reduce User's Permissions**
- **Verify Backups of ALL Data**
- **Verify Backups can be Restored**
- **Air-gapped Backups**
- **Prepared & Tested Manual Processes**
- Policies, Procedures, Evidence
- Insurance



Know Your Insurance

- Do you have **CHOICE**?
- Know your:
 - Legal
 - Forensics
 - Crisis Communications/PR
- Have your vendors Pre-Approved before you need them



January 14, 2020 - just 5 weeks from now

- Windows 7 Professional End-of-Life
- Windows Server 2008 R2 End-of-Life
- Replace all old computers or...
- Buy Microsoft Extended Support

F. Paul Greene
fgreene@hselaw.com
www.hselaw.com

Mike Semel
mike@semelconsulting.com
www.semelconsulting.com



www.semelconsulting.com/arccheckup/