EXCLUSIVELY FOR

The Arc New York

What the FBI Didn't Tell You

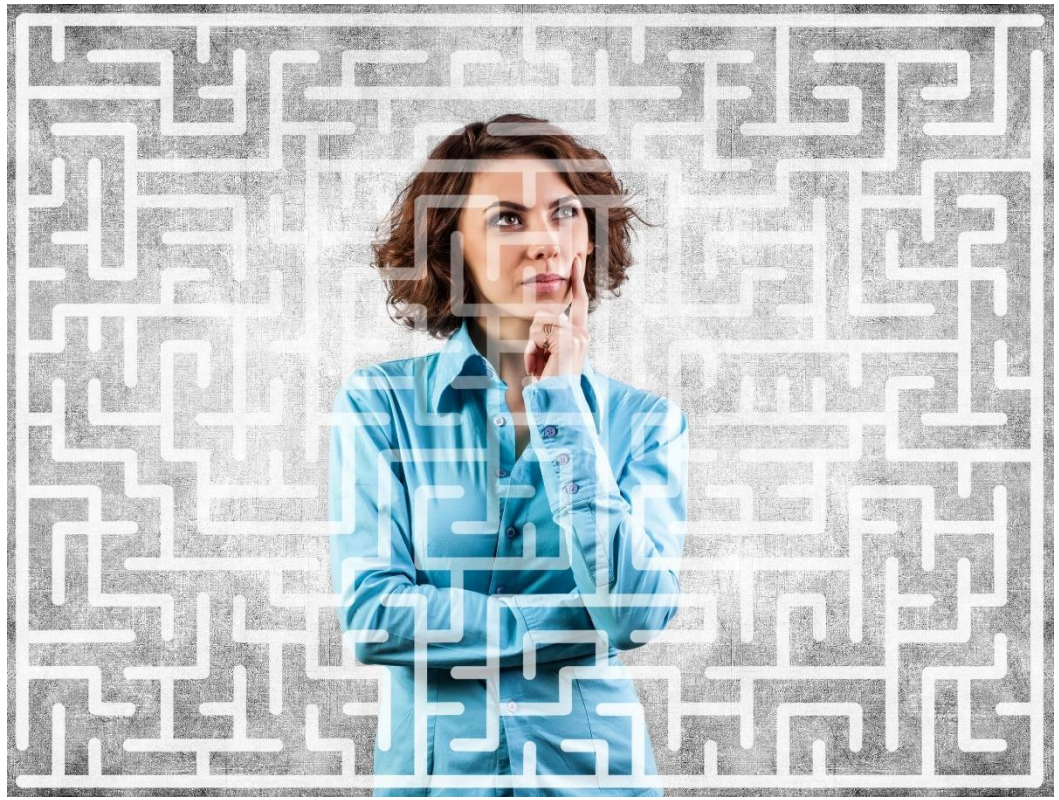
The Non-technical CEO's Guide to Ransomware & Email Scams

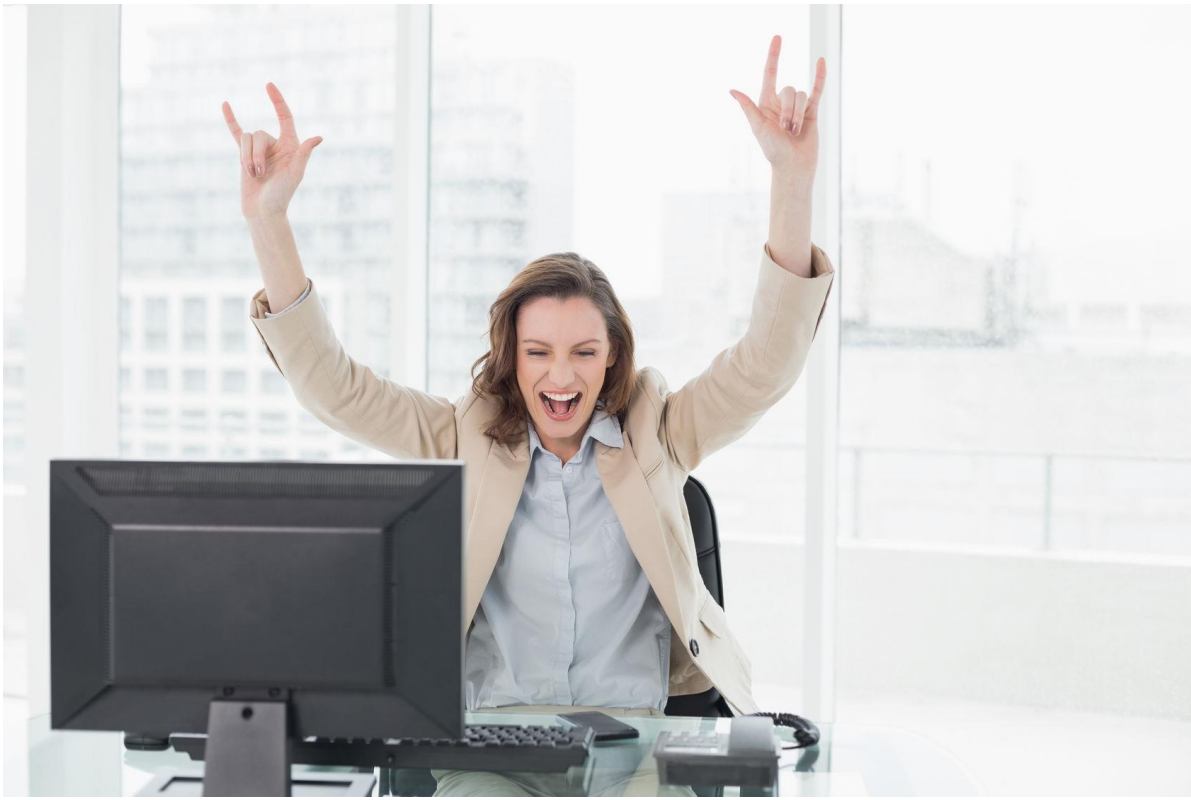
This webinar should not be considered legal advice.

Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

We want you to move from WONDERING to CONFIDENT





F. Paul Greene, Esq.

Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

- 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

Ponemon INSTITUTE

TOP RANKED USA CHAMBERS AND PARTNERS 2018

HSE

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

New York Law Journal

Outside Counsel — Expert Analysis

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

New York Law Journal

Outside Counsel — Expert Analysis

New Regulations Add to Complexity Of Cybersecurity Compliance

New York Law Journal

Corporate Update

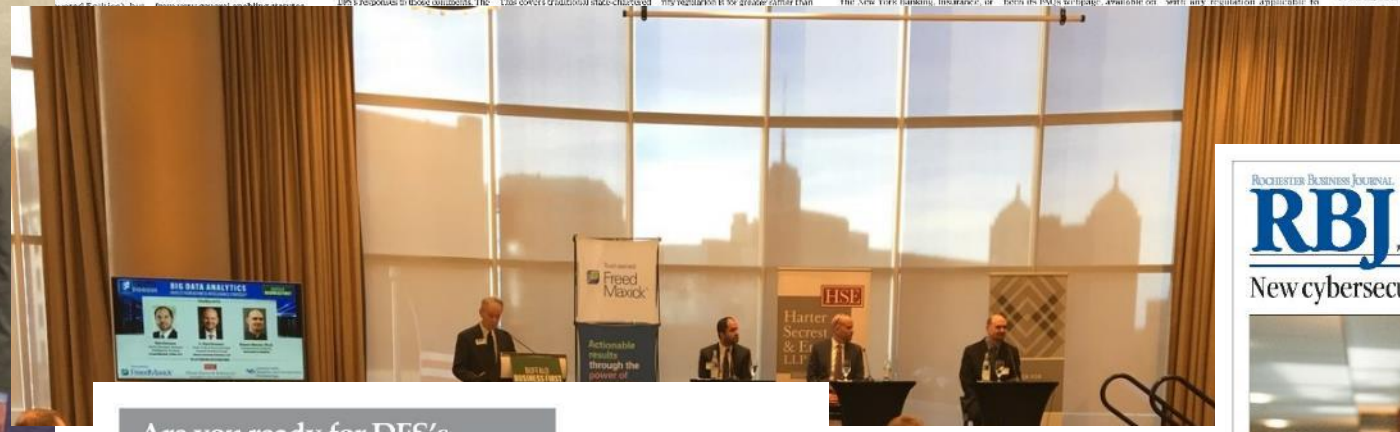
FINANCIAL SERVICES

NY DFS Issues Sweeping FAQs Affecting Scope of Regulations

New York Law Journal

Outside Counsel — Expert Analysis

The Equifax Breach: Why This One Is Different



Are you ready for DFS's new cybersecurity regulations?

DISTINGUISHED FELLOW

Ponemon Institute

This Certificate confers the honors and privileges of serving as a Distinguished Fellow of Ponemon Institute

E Paul Greene

In recognition of your service, commitment and leadership to the advancement of responsible information management practices in business and government.

HSE

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

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

VOLUME 32, NUMBER 32 — WWW.RBJDAILY.COM — NOVEMBER 11, 2016

New cybersecurity regulations need clarification

The state has placed a great deal of emphasis on the need for cybersecurity regulations, but some 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 LIVADAS

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

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

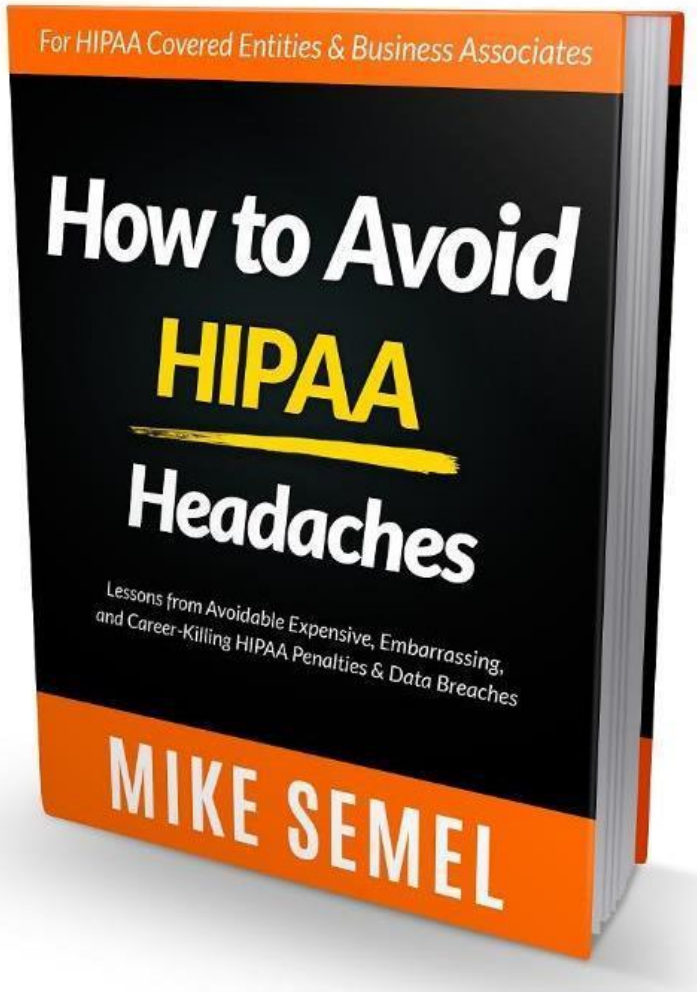
SEMEL CONSULTING

Speaking, Writing

Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

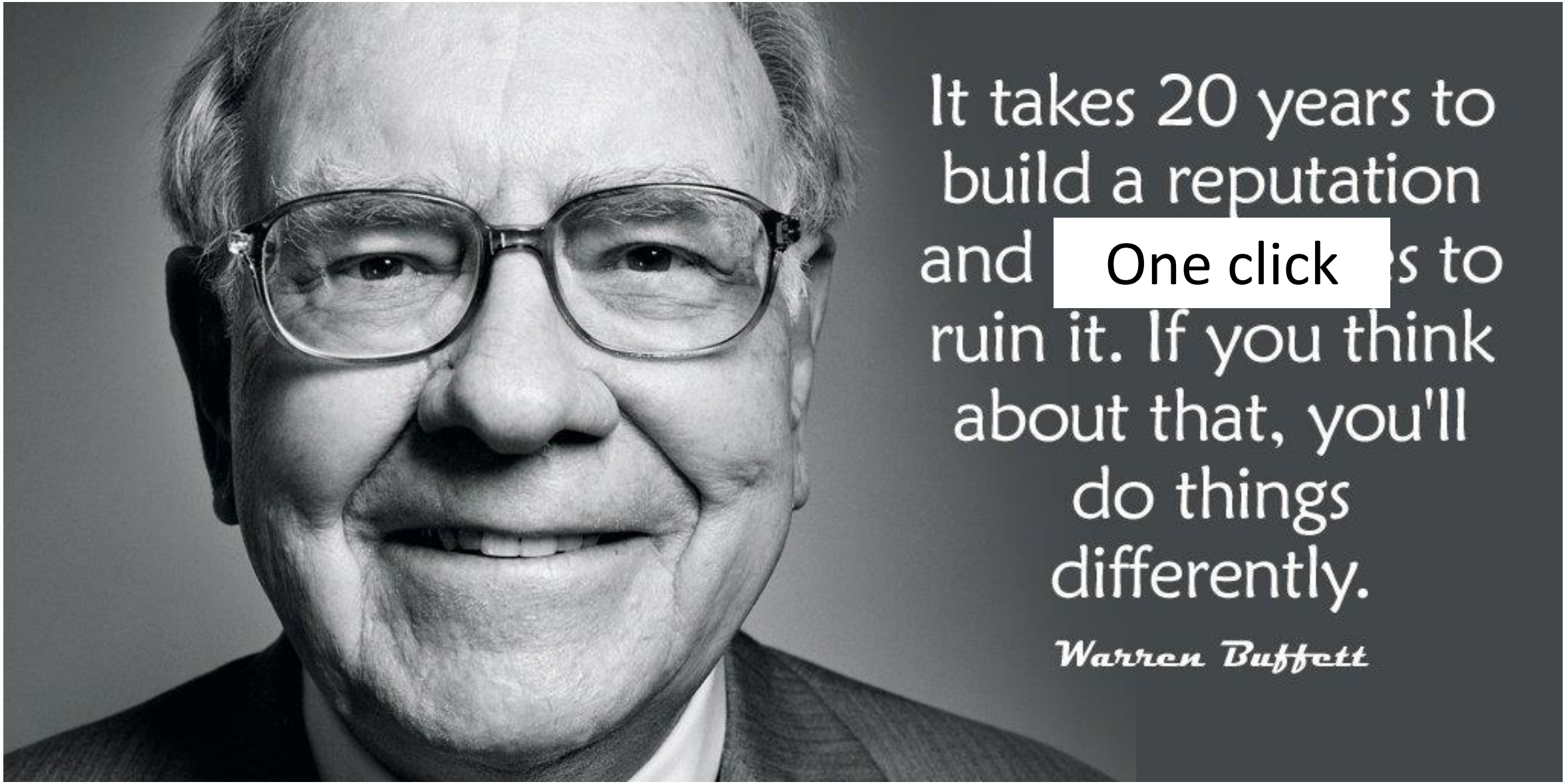
Amazon Best-Seller



Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

Cyber Security
Is a BUSINESS problem
With a TECHNICAL solution



Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

2019 FBI Cyber Warnings

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

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

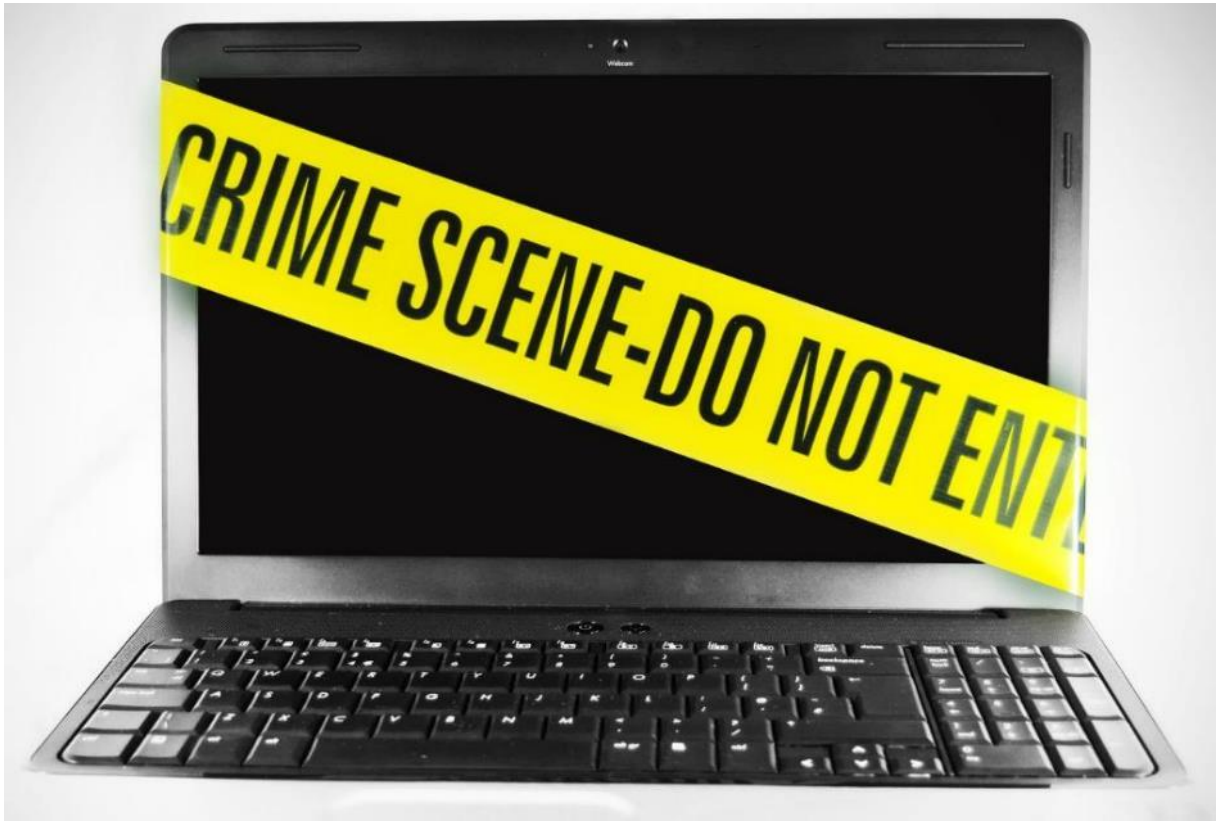
Business Email Compromise

Email ‘from ‘the boss’

- Funds Transfer
- Payroll Information
- Gift Card Purchase

Email ‘from an employee’

- Direct Deposit Redirection

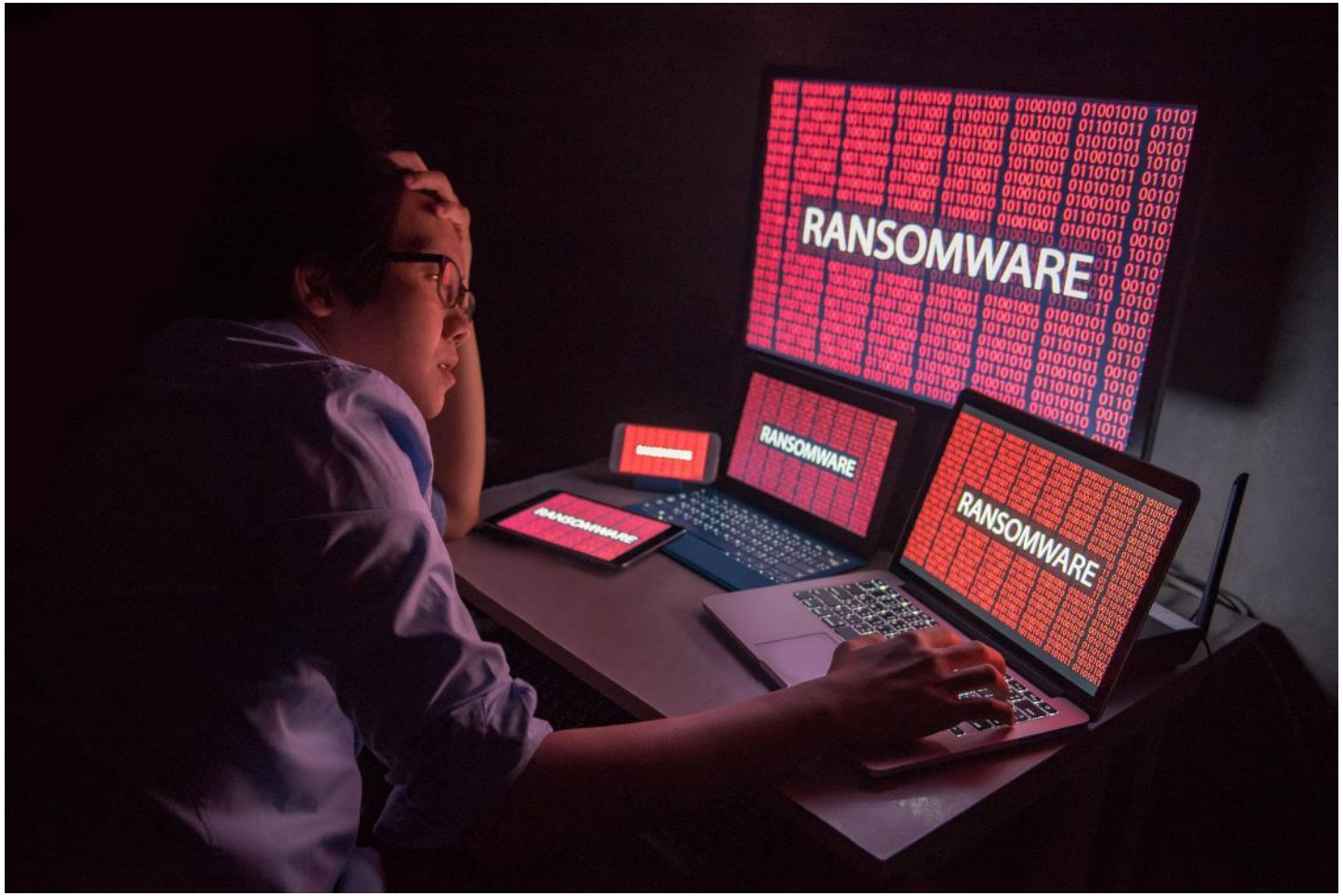


Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

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

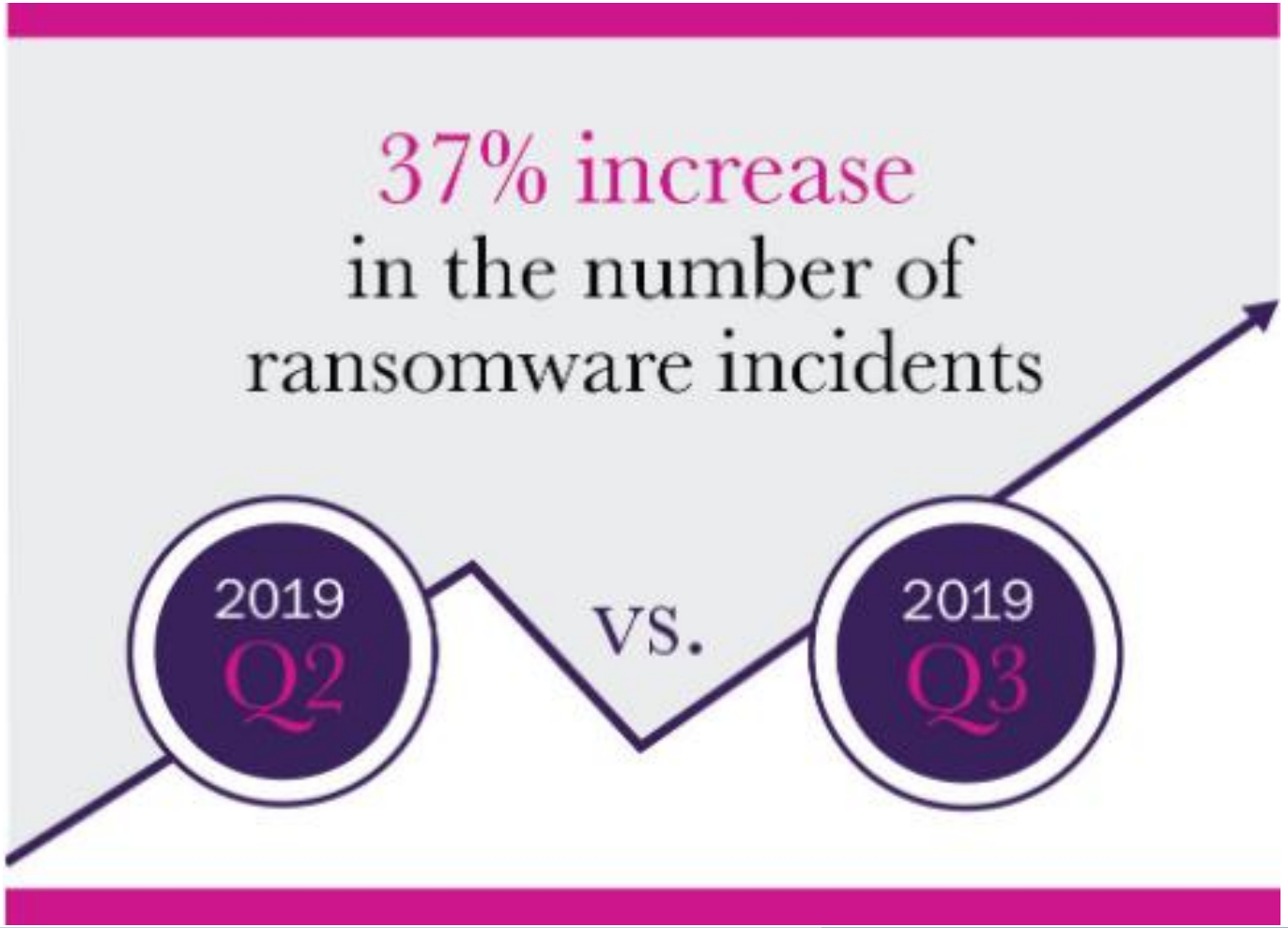
Ransomware Growth

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

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."*

Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING

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-Secrest

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-Secrest

Insurance

Incident Response

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

First Party Coverages

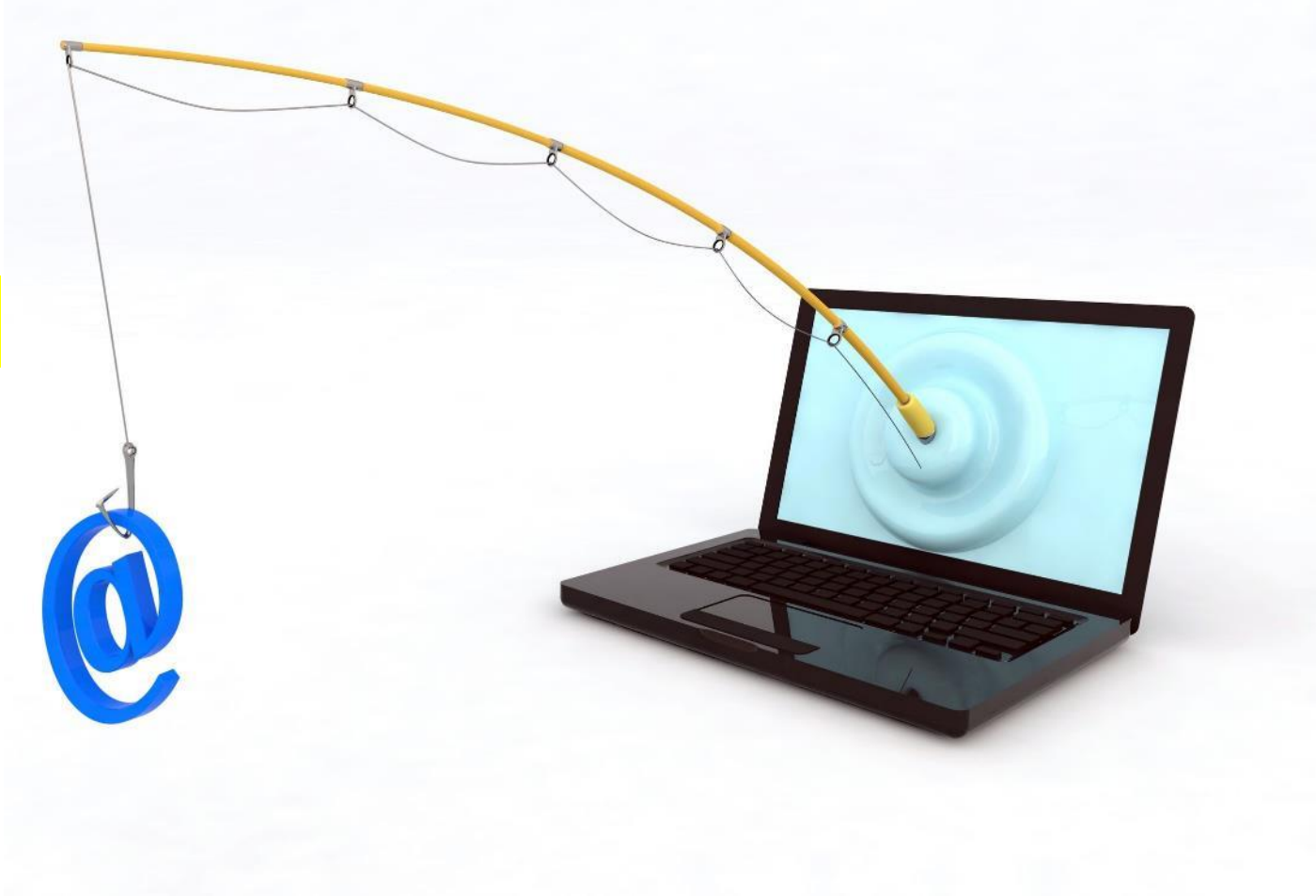
- Business Interruption
- Contingent Business Interruption
- Extortion
- Digital Data Recovery
- Financial Fraud
- Telecom Fraud

Third Party Coverages

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

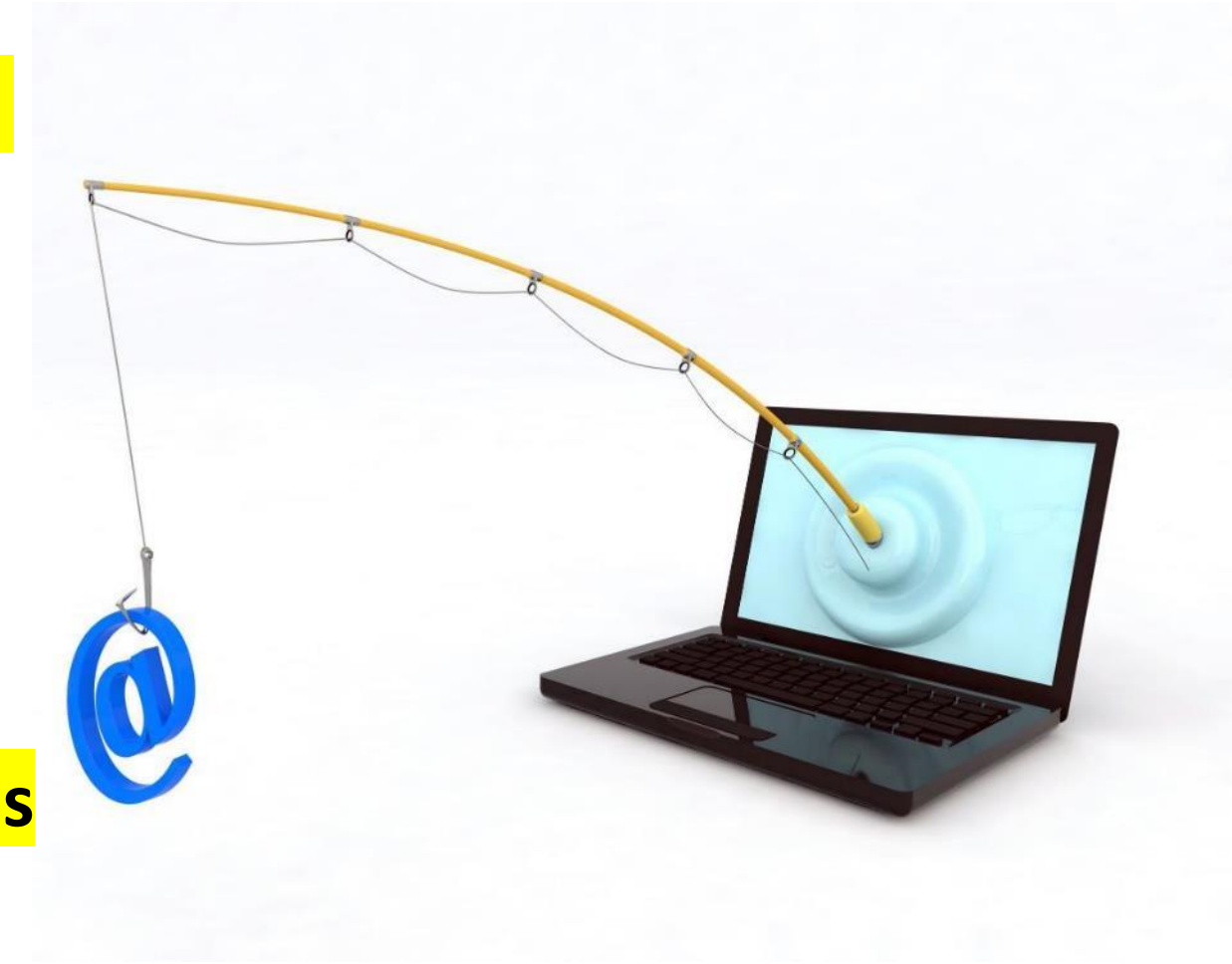
Strategies to Protect Against Business E-Mail Compromise

- **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

SEMEL CONSULTING

www.semelconsulting.com/arccheckup/

Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS
ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY

SEMEL CONSULTING