The 28th National HIPAA Summit

# Data is Worth More Than Gold

## Why Focusing on HIPAA May Be Your Biggest Mistake



SEMEL CONSULTING

# Mike Semel

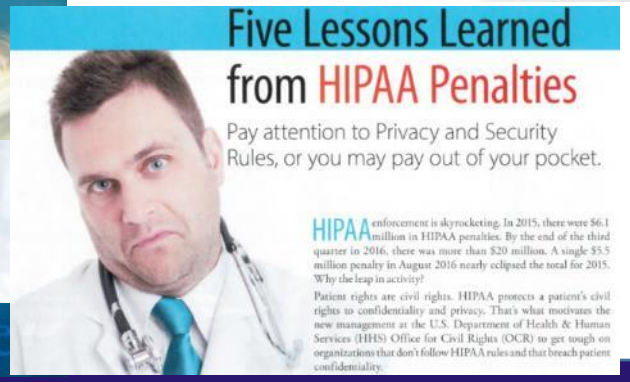
- 35-year IT business owner/manager
- 12 year certified HIPAA Professional
- EMT/ER Tech/FD Rescue Captain/IndyCar Safety Team
- Hospital/Skilled Nursing CIO
- School District CIO
- Cloud Backup Service COO

**Mike Semel**
**President**
**Chief Compliance Officer**
**SEMEL Consulting**

# Speaking, Writing





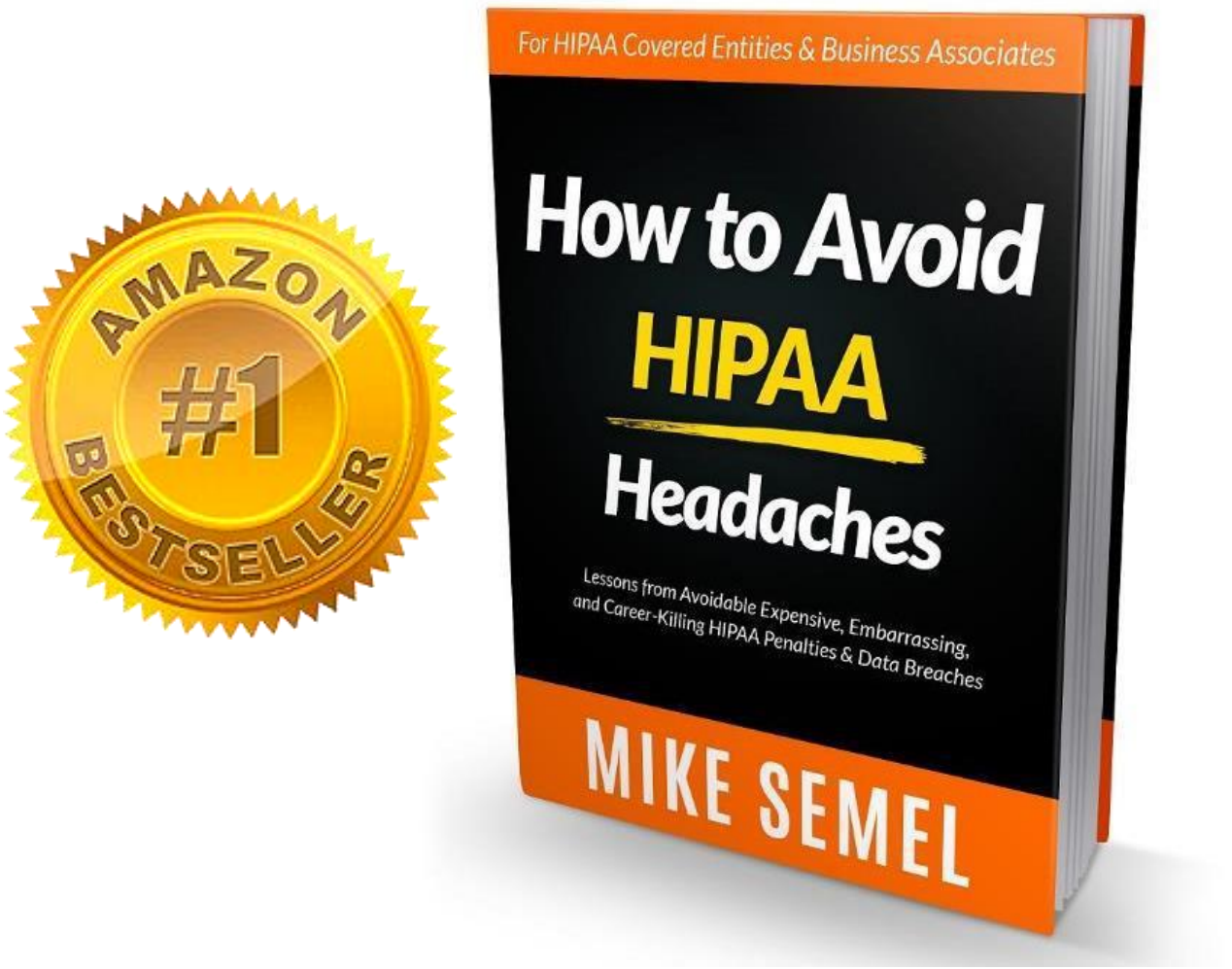






SEMEL CONSULTING

# Amazon Best-Seller



1. **Does your senior management treat HIPAA as a business risk?**

2. **Is HIPAA treated just as a compliance requirement to get out of the way?**

3. **Do you know the notification & reporting requirements in your state laws?**

4. **Do you know the requirements in your cyber liability insurance policy?**

5. **Do you know the requirements of any contracts or data use agreements your organization has signed?**

6. **Can you QUANTIFY your risks in DOLLARS to get the right resources?**

# What is Compliance?

Having to meet requirements set by others

- Federal & State Laws
- Industry Regulations
- Contractual Obligations
- Insurance Policy Requirements

# A COMPLIANCE HORROR STORY

# Patient Data Published to Internet

- Cottage Health's IT vendor installed a server and accidently published it to the Internet
- Patients Googled Themselves & Got their Medical Records
- IT Vendor did not have insurance so Cottage Health filed a claim with its cyber-liability carrier, Columbia Casualty
- Patients sued, lawsuit settled for $ 4.1 million
- Columbia Casualty paid settlement and lawyer's fees, but said it was still investigating…
- Columbia is sued Cottage Health to recover its $ 4.1 million

# 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.**

# State & Federal Penalties

HHS.gov
Health Information Privacy

## Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million

XAVIER BECERRA
*Attorney General*

**Attorney General Becerra Announces $2 Million Settlement Involving Santa Barbara-based Cottage Health System Over Failure to Protect Patient Medical Records**

- **Failed to conduct an accurate and thorough assessment of the potential risks**

  **Failed to implement security measures sufficient to reduce risks**
- **Failed to perform periodic technical and non-technical**
- **Failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.**

# For an error caused by a vendor…

- Lawsuit - $ 4,125,000
- California - $ 2,000,000
- OCR - $ 3,000,000

**TOTAL $ 9,125,000**

# Security is a BUSINESS problem
# With a TECHNICAL solution

# $ 9,125,000
# is a BUSINESS problem

# HIPAA Penalties

**2014 – 2015**

**$ 14 million**

**2016 – 2017**

**$ 42 million**

**2018**

**$ 28.7 million**

# Data Protection = Consumer Protection

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

## When The Government Closes Your Business

## The FTC's Data Security Error: Treating Small Businesses Like The Fortune 1000 Forbes

LabMD

Daugherty opened LabMD 18 years ago, in 1996. The lab operated as a small business of 20-some employees and

# Data Protection = Consumer Protection

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

## Stolen Laptop Leads to 20-Year FTC Oversight for Accretive Health

- Thursday, January 2nd, 2014 Print | Email

BECKER'S HOSPITAL REVIEW

| Accretive Stock Price | & | Market Cap |
|---|---|---|
| Before Breach | $ 30/share | $ 865 million |
| After Breach | $ 2/share | $ 197 million |



SEMEL CONSULTING

# Every business in ALL 50 states is regulated !!!

- ALL states, plus Washington, DC, Guam, Puerto Rico, & USVI
- Protect:
  - **Social Security Number**
  - **Driver's License Number** or state issued ID card
  - **Account number**, **credit or debit card** with access info
- 20 states protect **Medical Records** Beyond HIPAA
- States have shorter reporting deadlines
- You must comply with the laws protecting data on customers whose info you have, not just where you are

CANADA – PIPEDA
Alberta
British Columbia
Quebec

# Increased State Legislation

KPIX 5 CBS SF BayArea

## California Consumer Data Privacy Protections Expanded Under Proposed Law

February 25, 2019 at 3:16 pm **Filed Under:** Attorney General Xavier Becerra, California, California Senate, Consumer Privacy Act, Data Breach, Identity theft, Privacy, SB 561

SACRAMENTO (CBS SF/AP) — California consumers would have more power to sue corporations for misusing their data under a proposal to expand what already is the nation's most far-reaching law protecting personal information.

## Sweeping New Colorado Data Privacy Law Impacts Health Care Industry

LEXOLOGY.

## Delaware Passes Amendment to Data Breach Notification Law ...

# Breach Notification Laws

HIPAA - Breaches over 500 records report without unreasonable delay or a maximum of 60 days

California requires 15-day notification

# Increased Litigation

COHELAN KHOURY & SINGER
Leading Employment Rights and Consumer Protection Lawyers

## California Data Breach & Internet Privacy and Internet Fraud Lawyers

### Data Breach Issues

If you believe your private medical records, credit or debit card information, social security number, personal or financial information has been compromised, you should consult with lawyers qualified to advise you of your rights. Shoppers at Target, Neiman-Marcus, discount retailers, medical center



SEMEL CONSULTING

# Patient Lawsuits

## Then -

- **Medical Malpractice**
  - Medical Treatment
  - Complaint from 1 patient
  - Insurance coverage
  - Liability Limitations

## Now -

**Medical Malpractice**

- Data Breach
- Sued by ALL patients at same time?
- Insurance coverage ?
- Liability Limitations ?
- **$ 1.4 million jury award**

**Breach of Contract**

**Negligent Misrepresentation**

Court considered Notice of Privacy Practices a contract with patients

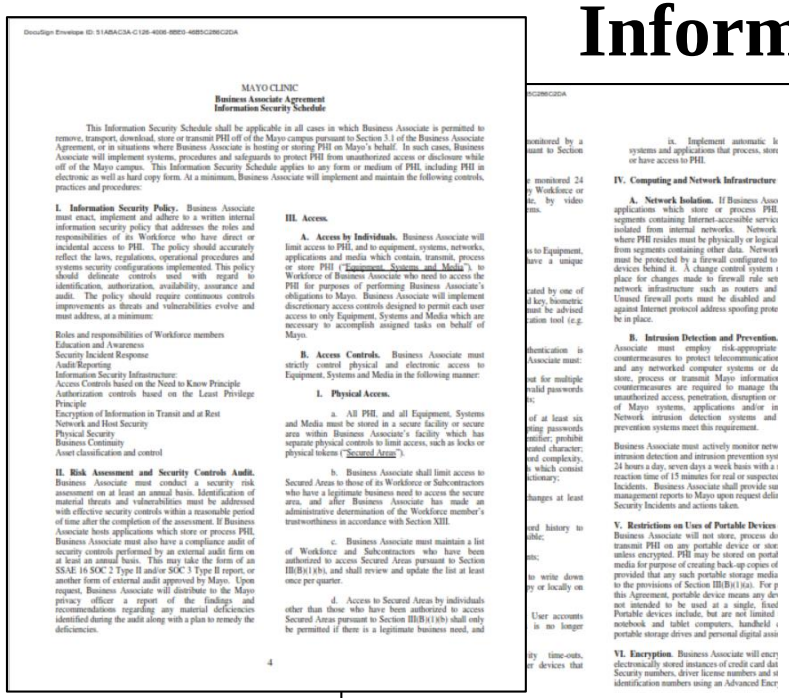
Complaint from ALL patients at same time

**$ 853,000 jury award**

# Contracts

MAYO CLINIC

## Business Associate Agreement
## Information Security Schedule



MAYO CLINIC
**Business Associate Agreement**
**Information Security Schedule**

This Information Security Schedule shall be applicable in all cases in which Business Associate is permitted to remove, transport, download, store or transmit PHI off of the Mayo campus pursuant to Section 3.1 of the Business Associate Agreement, or in situations where Business Associate is hosting or storing PHI on Mayo's behalf. In such cases, Business Associate will implement systems, procedures and safeguards to protect PHI from unauthorized access or disclosure while off of the Mayo campus. This Information Security Schedule applies to any form or medium of PHI, including PHI in electronic as well as hard copy form. At a minimum, Business Associate will implement and maintain the following controls, practices and procedures:

**I. Information Security Policy.** Business Associate must enact, implement and adhere to a written internal information security policy that addresses the roles and responsibilities of its Workforce who have direct or incidental access to PHI. The policy should accurately reflect the laws, regulations, operational procedures and systems security configurations implemented. This policy should delineate controls used with regard to identification, authorization, availability, assurance and audit. The policy should require continuous controls improvements as threats and vulnerabilities evolve and must address, at a minimum:

Roles and responsibilities of Workforce members
Education and Awareness
Security Incident Response
Audit/Reporting
Information Security Infrastructure:
Access Controls based on the Need to Know Principle
Authorization controls based on the Least Privilege Principle
Encryption of Information in Transit and at Rest
Network and Host Security
Physical Security
Business Continuity
Asset classification and control

**II. Risk Assessment and Security Controls Audit.** Business Associate must conduct a security risk assessment on at least an annual basis. Identification of material threats and vulnerabilities must be addressed with effective security controls within a reasonable period of time after the completion of the assessment. If Business Associate hosts applications which store or process PHI, Business Associate must also have a compliance audit of security controls performed by an external audit firm on at least an annual basis. This may take the form of an SSAE 16 SOC 2 Type II and/or SOC 3 Type II report, or another form of external audit approved by Mayo. Upon request, Business Associate will distribute to the Mayo privacy officer a report of the findings and recommendations regarding any material deficiencies identified during the audit along with a plan to remedy the deficiencies.

**III. Access.**

**A. Access by Individuals.** Business Associate will limit access to PHI, and to equipment, systems, networks, applications and media which contain, transmit, process or store PHI ("Equipment, Systems and Media"), to Workforce of Business Associate who need to access the PHI for purposes of performing Business Associate's obligations to Mayo. Business Associate will implement discretionary access controls designed to permit each user access to only Equipment, Systems and Media which are necessary to accomplish assigned tasks on behalf of Mayo.

**B. Access Controls.** Business Associate must strictly control physical and electronic access to Equipment, Systems and Media in the following manner:

**1. Physical Access.**

a. All PHI, and all Equipment, Systems and Media must be stored in a secure facility or secure area within Business Associate's facility which has separate physical controls to limit access, such as locks or physical tokens ("Secured Areas").

b. Business Associate shall limit access to Secured Areas to those of its Workforce or Subcontractors who have a legitimate business need to access the secure area, and after Business Associate has made an administrative determination of the Workforce member's trustworthiness in accordance with Section XIII.

c. Business Associate must maintain a list of Workforce and Subcontractors who have been authorized to access Secured Areas pursuant to Section III(B)(1)(b), and shall review and update the list at least once per quarter.

d. Access to Secured Areas by individuals other than those who have been authorized to access Secured Areas pursuant to Section III(B)(1)(b) shall only be permitted if there is a legitimate business need, and

4

ix. Implement automatic l
systems and applications that process, stor
or have access to PHI.

**IV. Computing and Network Infrastructure**

**A. Network Isolation.** If Business Asso
applications which store or process PHI,
segments containing Internet-accessible servic
isolated from internal networks. Network
where PHI resides must be physically or logical
from segments containing other data. Network
must be protected by a firewall configured to
devices behind it. A change control system
place for changes made to firewall rule set
network infrastructure such as routers and
Unused firewall ports must be disabled and
against Internet protocol address spoofing prote
be in place.

**B. Intrusion Detection and Prevention.**
Associate must employ risk-appropriate
countermeasures to protect telecommunicatio
and any networked computer systems or da
store, process or transmit Mayo informatio
countermeasures are required to manage th
unauthorized access, penetration, disruption or
of Mayo systems, applications and/or in
Network intrusion detection systems and
prevention systems meet this requirement.

Business Associate must actively monitor netw
intrusion detection and intrusion prevention sys
24 hours a day, seven days a week basis with a
reaction time of 15 minutes for real or suspecte
Incidents. Business Associate shall provide su
management reports to Mayo upon request deli
Security Incidents and actions taken.

**V. Restrictions on Uses of Portable Devices**
Business Associate will not store, process do
transmit PHI on any portable device or stor
unless encrypted. PHI may be stored on portal
media for purpose of creating back-up copies of
provided that any such portable storage media
to the provisions of Section III(B)(1)(a). For p
this Agreement, portable device means any de
not intended to be used at a single, fixed
Portable devices include, but are not limited
notebook and tablet computers, handheld
portable storage drives and personal digital assi

**VI. Encryption.** Business Associate will encry
electronically stored instances of credit card dat
Security numbers, driver license numbers and s
identification numbers using an Advanced Encr

5

Documentat
information
responsible.

**II. Risk Assessment and Security Controls Audit.** Business Associate must conduct a security risk assessment on at least an annual basis. Identification of material threats and vulnerabilities must be addressed with effective security controls within a reasonable period of time after the completion of the assessment. If Business Associate hosts applications which store or process PHI, Business Associate must also have a compliance audit of security controls performed by an external audit firm on at least an annual basis. This may take the form of an

# Data Use Agreements

TEXAS
Health and Human Services

DATA USE AGREEMENT

**ARTICLE 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS**

a. For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Client Information, within the first, consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after

# Incident Management Plan

- **Know what your insurance company requires for coverage**
  - Audit your Insurance Policy Compliance
  - Immediately involve a cyber & compliance attorney
  - Get pre-approval for forensic & compliance specialists
  - Are you required to notify law enforcement?
- **Include all reporting requirements**
  - Federal, state, contractual

# Be ready to respond

The 28th National HIPAA Summit

# Data is Worth More Than Gold

## Translating Risk into Dollars

# Medical Record Black Market

- **Credit Card Number**



**25¢ - $1**



**$10 - $50**

- **Medical Record**



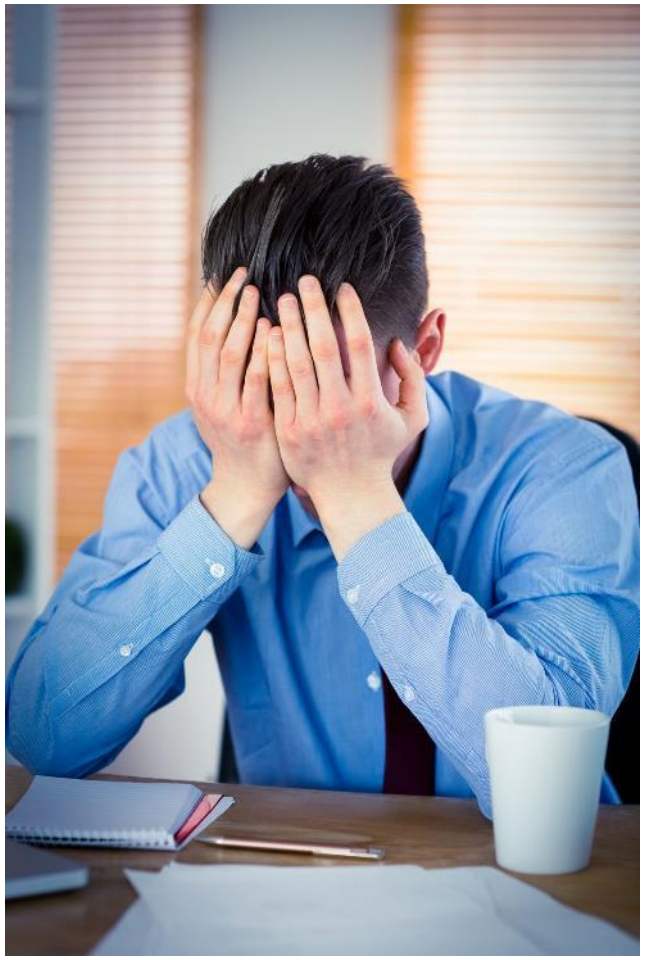

SEMEL CONSULTING

# 2018 Cost of a Data Breach Report

**$ 231** **Per Record**

**Across All Industries**

**$ 408** **Per Medical Record**



Source: 2018 Ponemon Cost of a Data Breach Report

**10,000 records -- $ 2- $ 4 million**

**25,000 records -- $ 5 - $ 10 million**

**100,000 records -- $ 20 – $ 40 million**

# Data is Worth More Than Gold

# Lost Thumb Drives

Thumb Drive Weight – ¾ of one ounce

Gold = $ 1200 per ounce

**If Thumb Drive was solid gold it would be worth $ 995**

A medical practice paid a **$ 150,000** fine when it lost a thumb drive containing patient records

A health plan paid **$ 2.2 million** when it lost a thumb drive

Data Worth $ 150,000
To $ 2.2 million

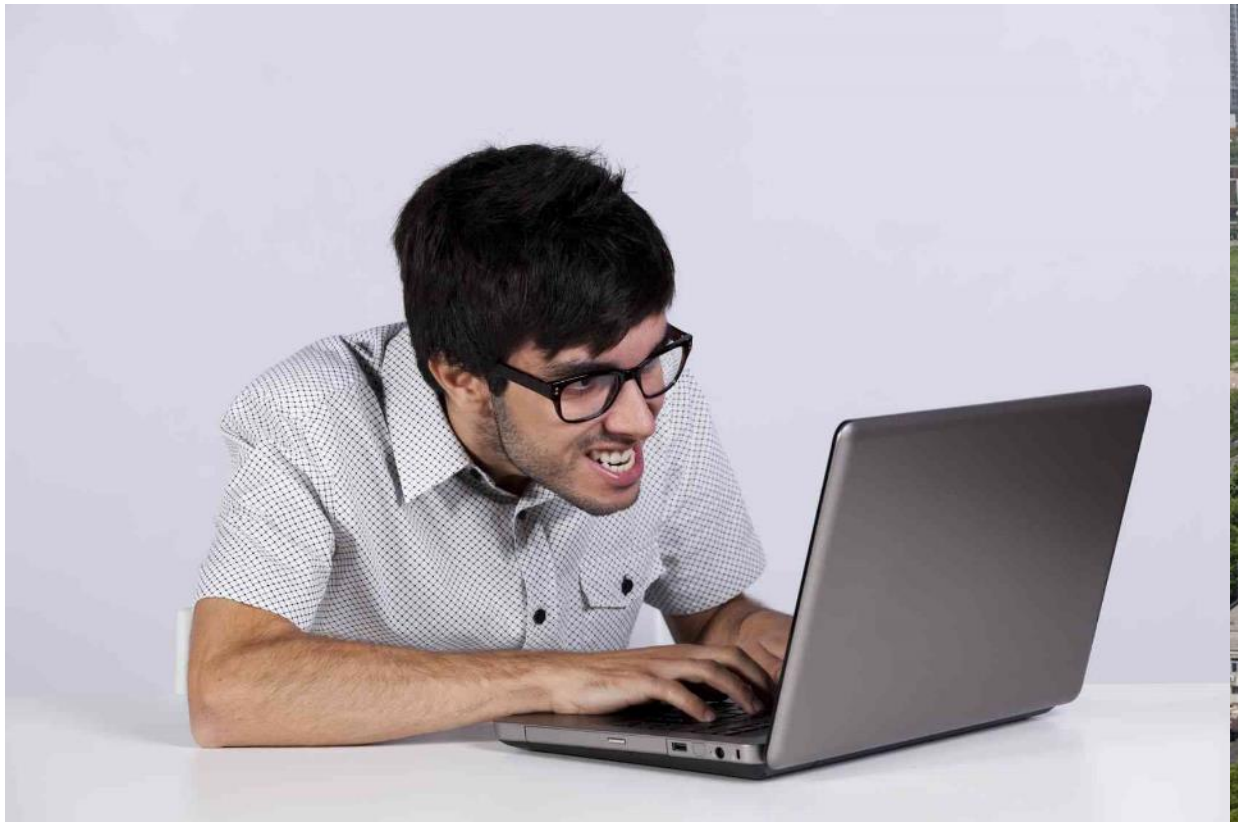
# Data is EVERYWHERE





# Threats Have Changed

## Then

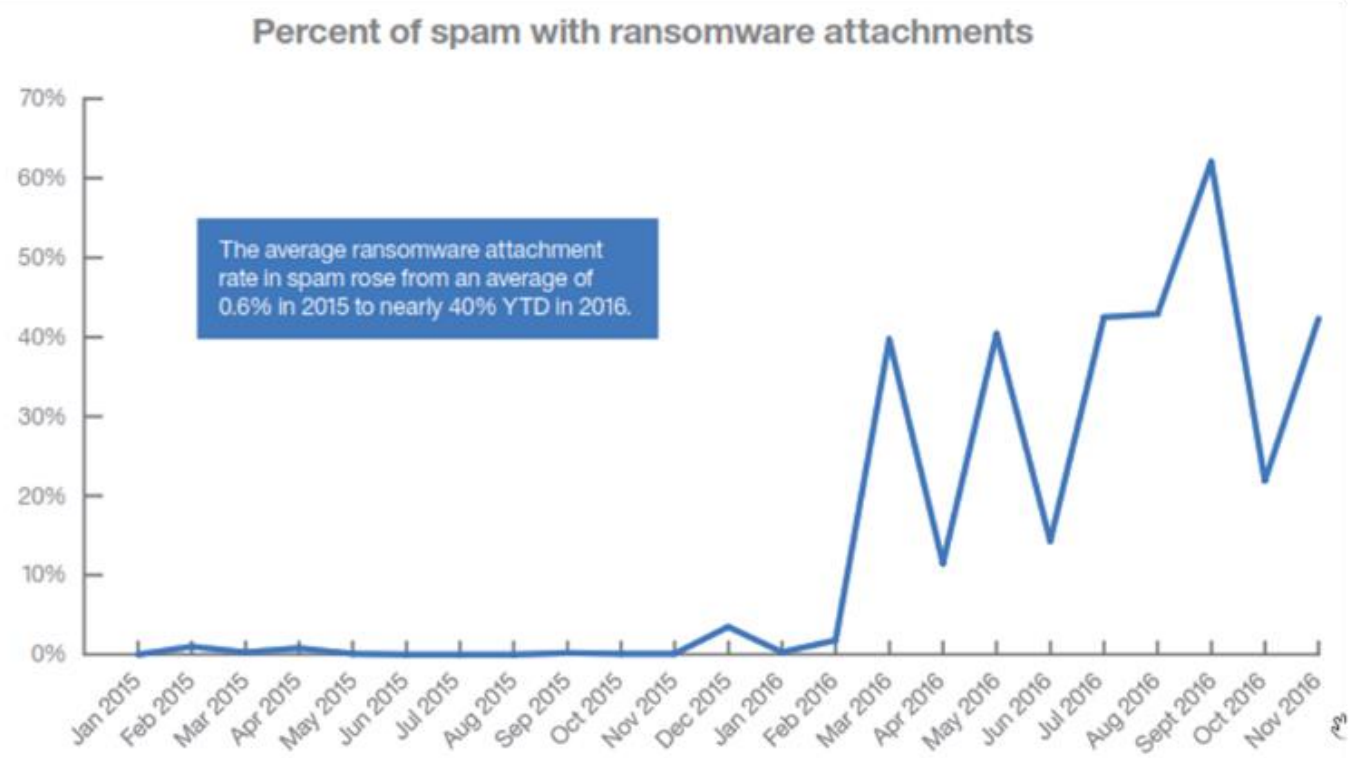


## Now

# Security Is More Important Now

IBM Security

**Ransomware increased 6,000 percent in 2016**




Per the IBM survey, seven in ten of those who have experience with ransomware attacks (70 percent) have paid to get data back. Resolution has come at a hefty price for some, with more than half paying over $10,000.

- 20 percent paid more than $40,000
- 25 percent paid $20,000 – $40,000
- 11 percent paid $10,000 – $20,000



SEMEL CONSULTING

# January 14, 2020

- Windows 7 Professional End-of-Life
- Windows Server 2008 R2 End-of-Life

- Budget Now
  - New Computers & Servers → New Operating Systems
- Plan Long Replacement Projects
  - **120 computers x 2 hours = 240 hours**
  - **15 servers x 3 hours = 45 hours**
  - **Total Replacement project = 285 hours/40 hours = 7 weeks**