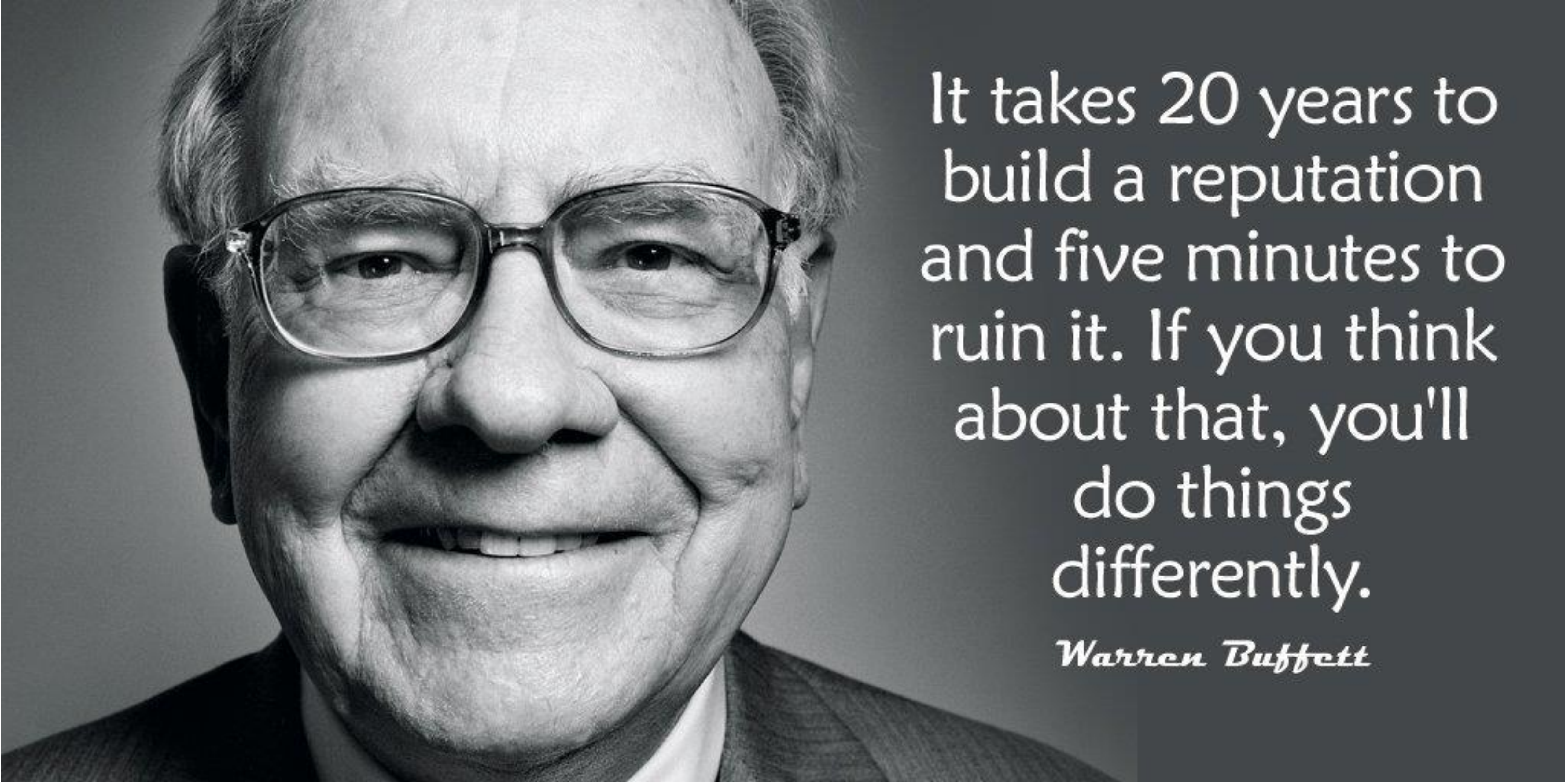
The 29th National HIPAA Summit

Finding & Fixing Hidden Cyber Risks



It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.

Warren Buffett

Mike Semel

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

Healthcare Tech OUTLOOK

HEALTHCARE COMPLIANCE SERVICES EDITION

SEMEL CONSULTING

ALL-INCLUSIVE SERVICE SUITE FOR HEALTHCARE COMPLIANCE

Mike Semel
President
Chief Compliance Officer
SEMEL Consulting

INFRAGARD PARTNERSHIP FOR PROTECTION

Certified HIPAA 4Med approved Professional

CHP Certified HIPAA Professional HIPAA Academy

CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST

CERTIFIED BUSINESS CONTINUITY PROFESSIONAL DRI CBCP

CompTIA SECURITY TRUSTMARK+

Speaking , Writing

March-April 2016

Journal of Health Care Compliance

Balance Guide

Implementation of MIPS and APMs: Provider Compliance Considerations in the New World of Physician Payment Reform

Physician Value-Based Payment Impacts All Physicians 2016-2017

Why Security and Compliance Are Executive Responsibilities

Generic Drug Inflation Fallout: Rising Tide

HEALTHCARE BUSINESS MONTHLY

Five Lessons Learned from HIPAA Penalties

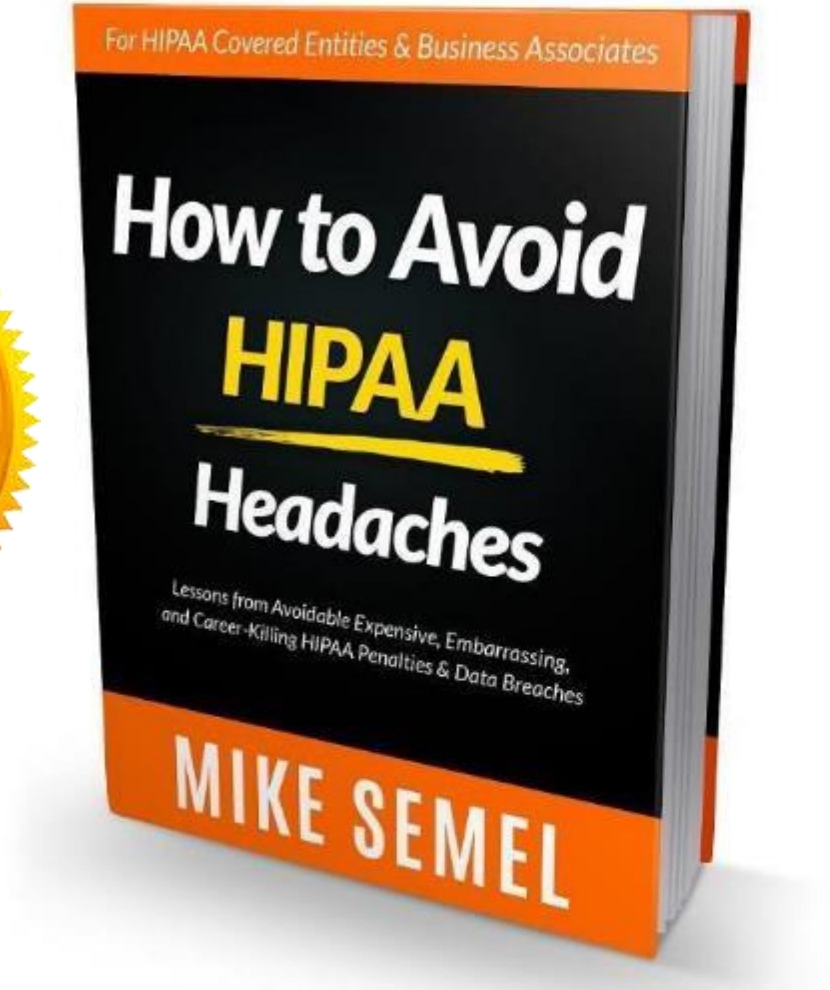
Pay attention to Privacy and Security Rules, or you may pay out of your pocket.

HIPAA enforcement is skyrocketing. In 2015, there were $6.1 million in HIPAA penalties. By the end of the third quarter in 2016, there was more than $20 million. A single $5.5 million penalty in August 2016 nearly eclipsed the total for 2015. Why the leap in activity?

Patient rights are civil rights. HIPAA protects a patient's civil rights to confidentiality and privacy. That's what motivates the new management at the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) to get tough on organizations that don't follow HIPAA rules and that breach patient confidentiality.

Why Security and Compliance Are Executive Responsibilities

Amazon Best-Seller


For HIPAA Covered Entities & Business Associates
How to Avoid
HIPAA
Headaches
Lessons from Avoidable Expensive, Embarrassing, and Career-Killing HIPAA Penalties & Data Breaches
MIKE SEMEL

What is Compliance?

Having to meet requirements set by others

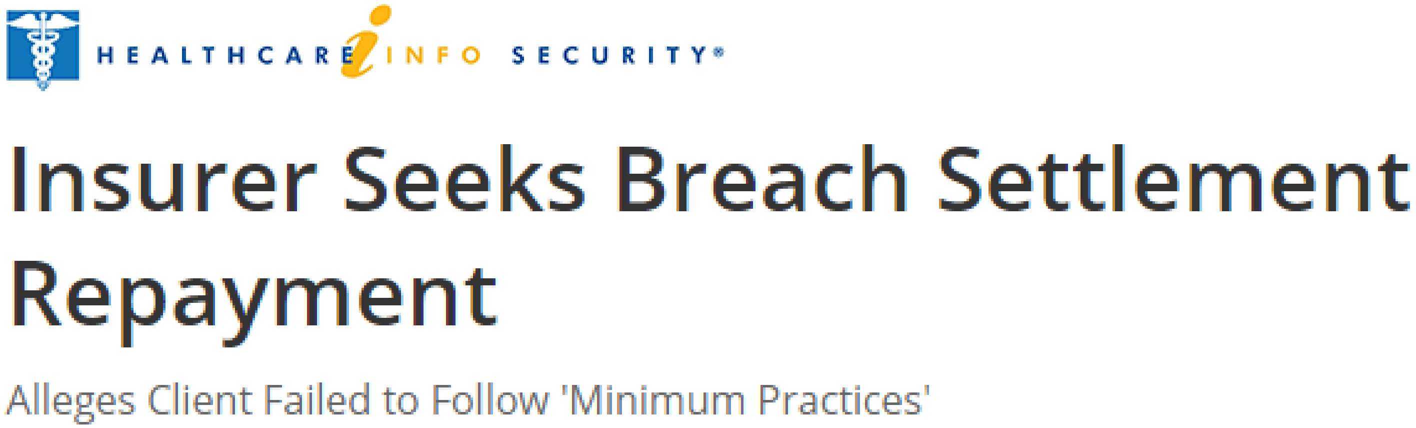
Federal & State Laws

Industry Regulations

Contractual Obligations

Insurance Policy Requirements

Will Your Cyber Liability Insurance Pay Off?



HEALTHCARE INFO SECURITY®

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.

2019 IBM Breach Report

IBM Security

Cost of a Data Breach Report 2019

July 2018 – April 2019 survey period

- Average cost of a data breach across all industries

$ 242 per record

- Average cost of a U.S. healthcare data breach

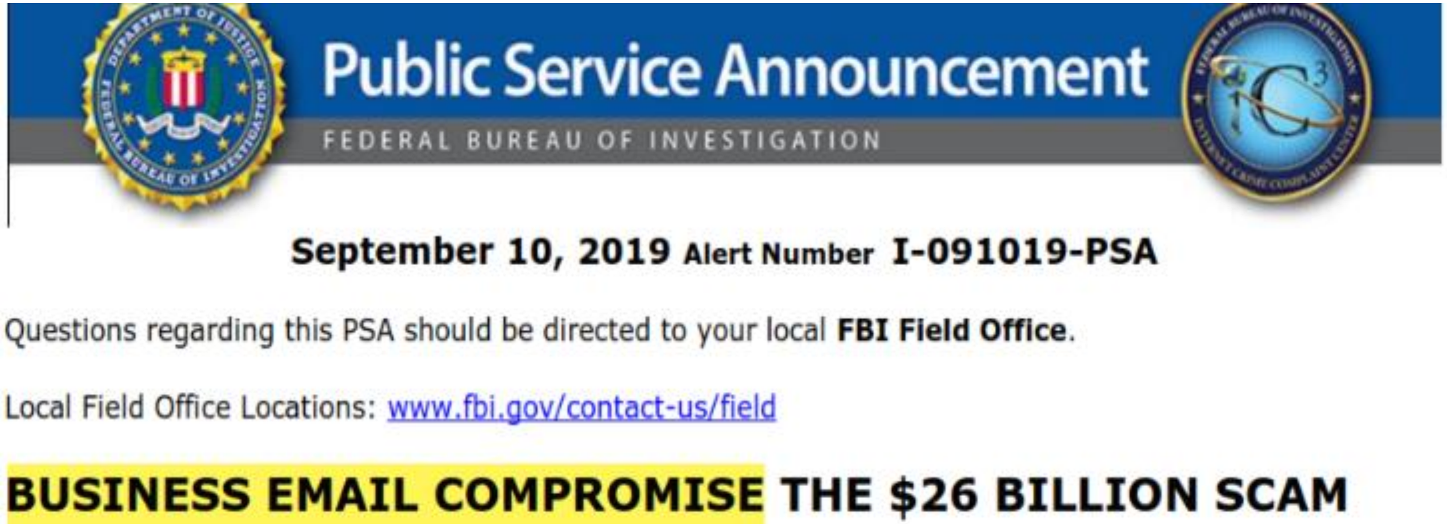
$ 429 per record

10,000 medical records -- $ 4.3 million

25,000 medical records -- $ 10 million

300,000 medical records -- $ 120 million

2019 FBI Cyber Warnings



Public Service Announcement

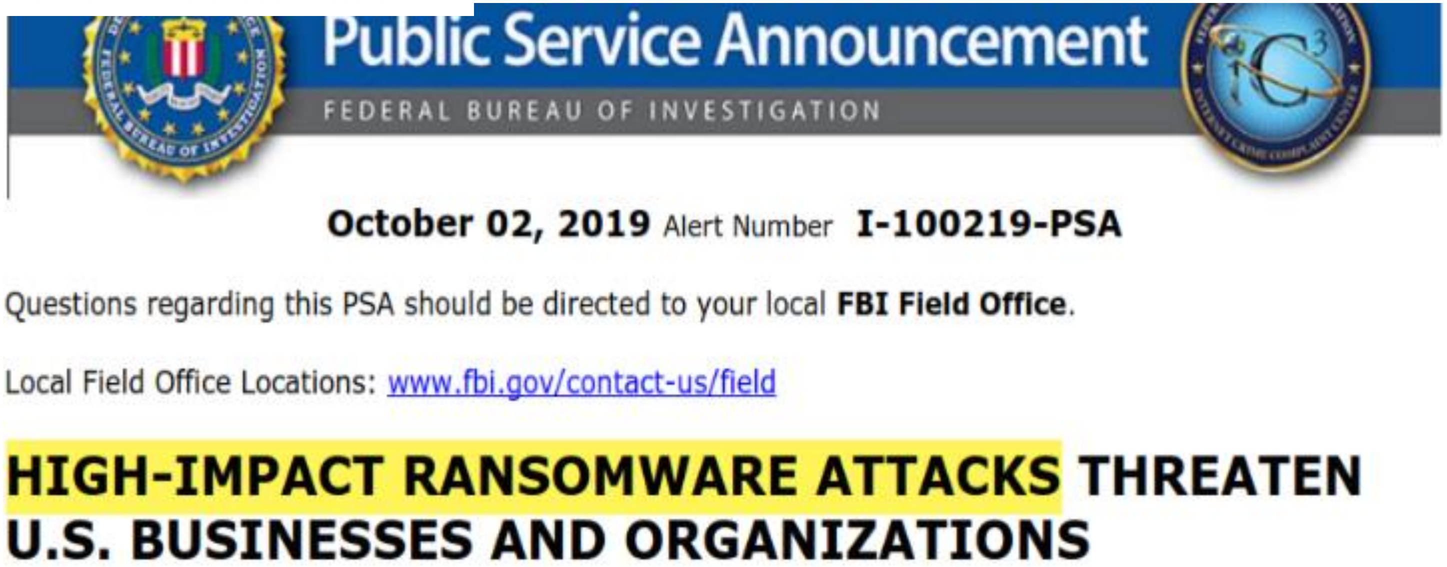
FEDERAL BUREAU OF INVESTIGATION

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

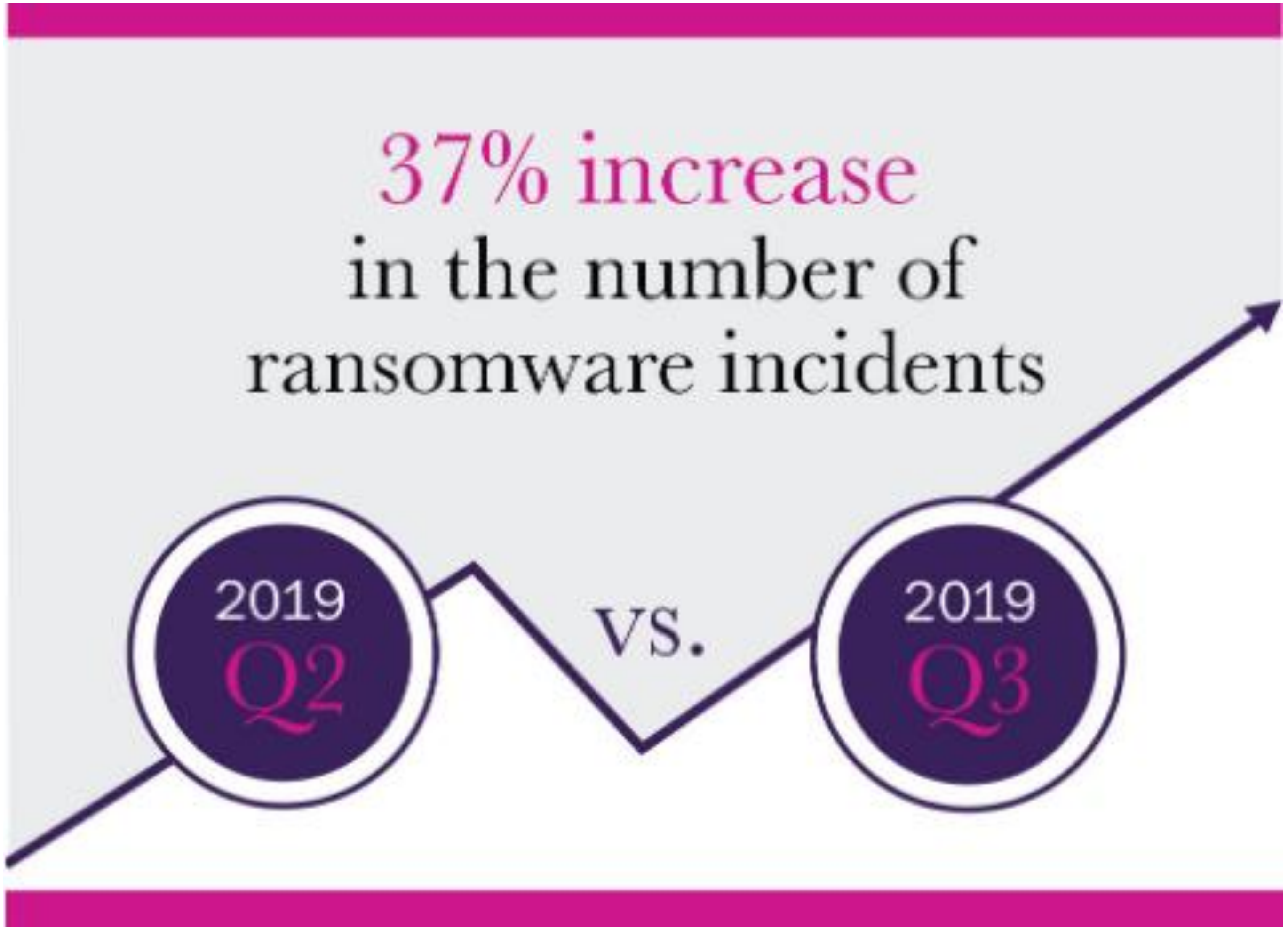
Email ‘from an employee’

- Direct Deposit Redirection

High-Impact Ransomware Deletes Backups

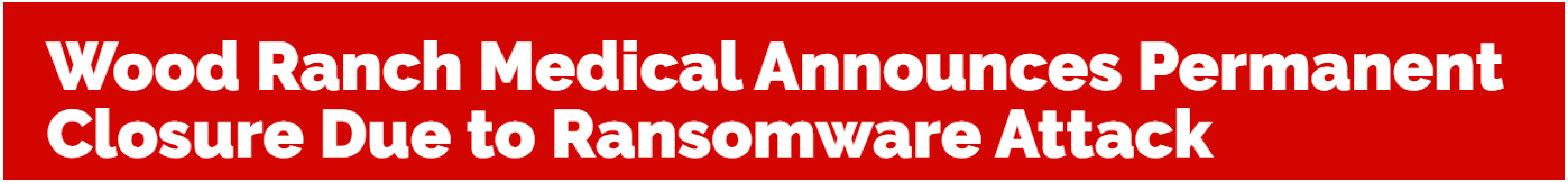
Security Is More Important Than Ever

Beazley breach insights - October 2019

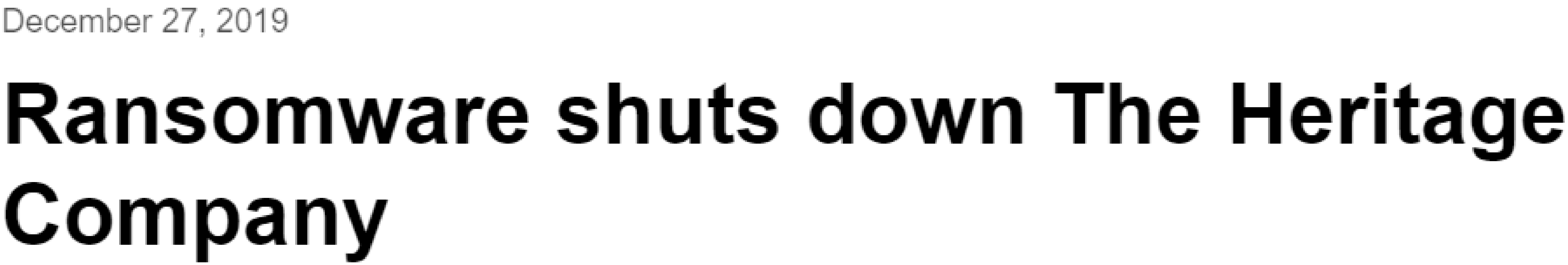


37% increase in the number of ransomware incidents

Cost of Ransomware



Wood Ranch Medical Announces Permanent Closure Due to Ransomware Attack



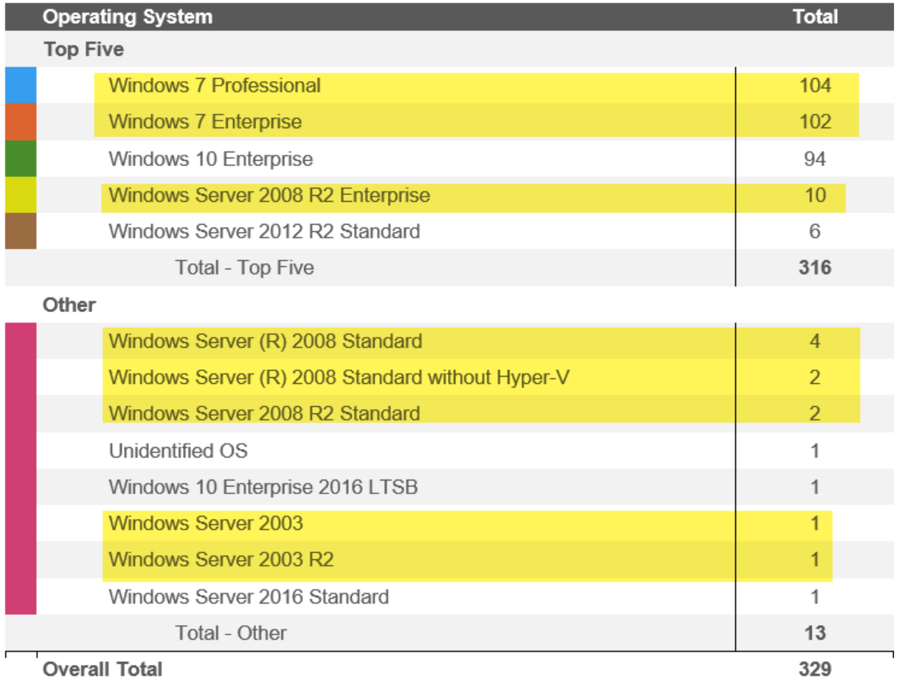
December 27, 2019

Ransomware shuts down The Heritage Company

Unsupported Software

- Windows 7 and older
- Windows Server 2008 and older
- SQL 2008 and older
- Old versions of Microsoft Office, Access, Crystal Reports, Acrobat, etc.

PC Upgrade Proiect



	Operating System	Total
	Top Five	
🟦	Windows 7 Professional	104
🟧	Windows 7 Enterprise	102
🟩	Windows 10 Enterprise	94
🟨	Windows Server 2008 R2 Enterprise	10
🟫	Windows Server 2012 R2 Standard	6
	Total - Top Five	**316**
	Other	
🟥	Windows Server (R) 2008 Standard	4
	Windows Server (R) 2008 Standard without Hyper-V	2
	Windows Server 2008 R2 Standard	2
	Unidentified OS	1
	Windows 10 Enterprise 2016 LTSB	1
	Windows Server 2003	1
	Windows Server 2003 R2	1
	Windows Server 2016 Standard	1
	Total - Other	**13**
	Overall Total	**329**

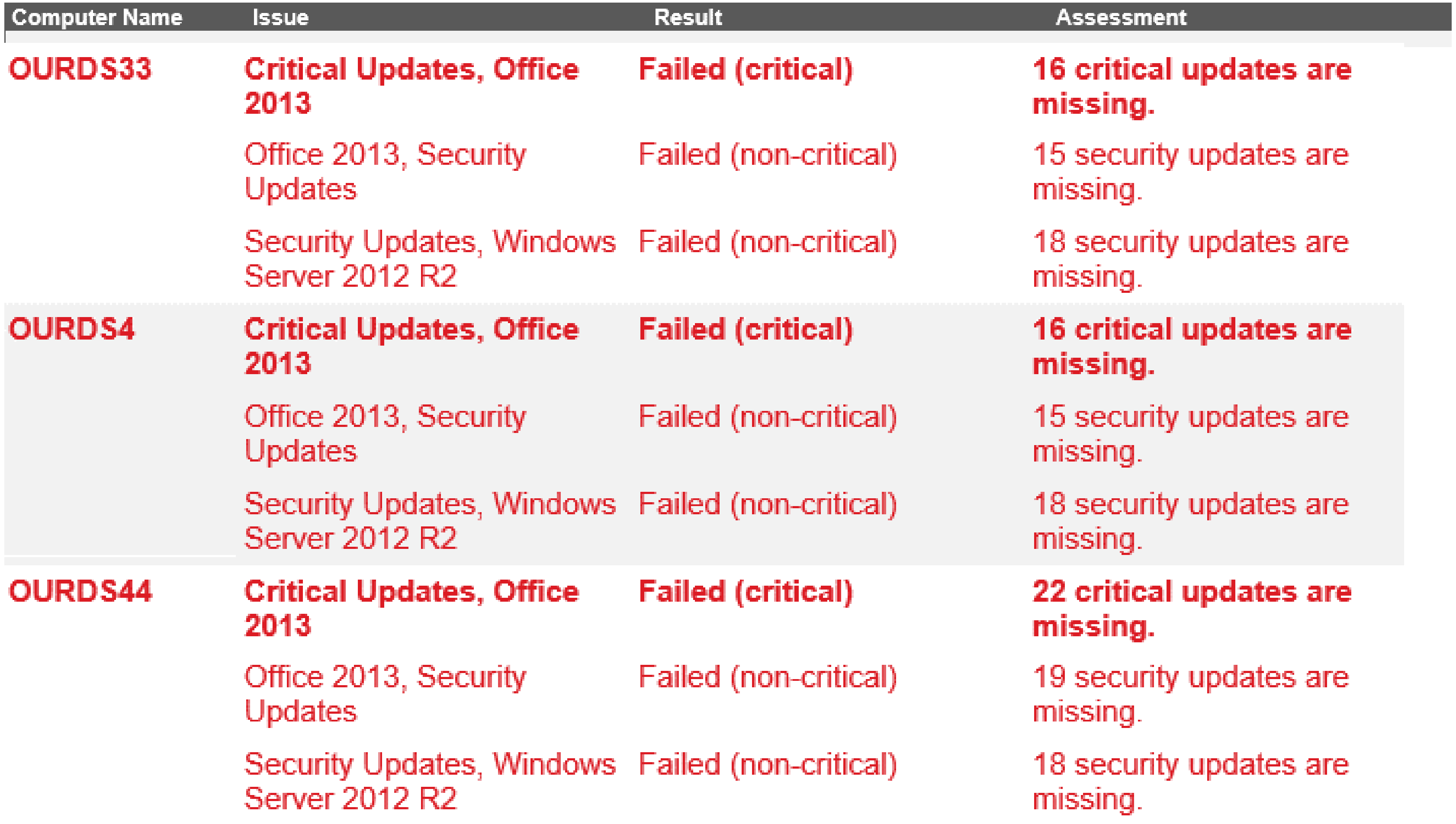
- **206 computers** x 2 hours/computer = 412 hours
- **18 Windows 2008 servers** x 3 hours/server = 54 hours
- **2 Windows 2003 servers** x 3 hours/server = 6 hours
- **472 hours/40 hour weeks = 11.8 weeks**

Users

- 37 Enabled users with Passwords set to never expire
- 241 Enabled users who have not logged in within the past 30 days
- 7 Enabled users with Generic User Names

Missing Critical Microsoft Patches

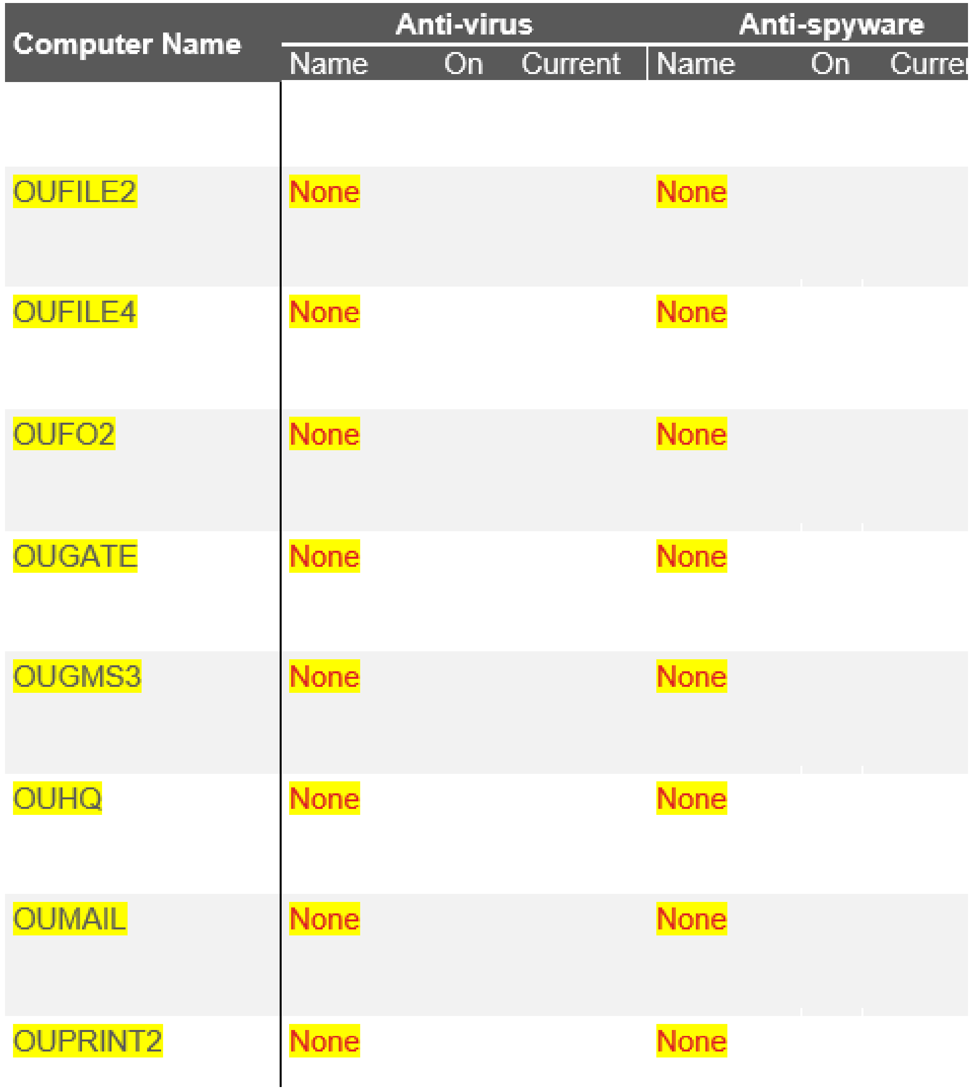
- 9 PC’s & Servers



Computer Name	Issue	Result	Assessment
OURDS33	**Critical Updates, Office 2013**	**Failed (critical)**	**16 critical updates are missing.**
	Office 2013, Security Updates	Failed (non-critical)	15 security updates are missing.
	Security Updates, Windows Server 2012 R2	Failed (non-critical)	18 security updates are missing.
OURDS4	**Critical Updates, Office 2013**	**Failed (critical)**	**16 critical updates are missing.**
	Office 2013, Security Updates	Failed (non-critical)	15 security updates are missing.
	Security Updates, Windows Server 2012 R2	Failed (non-critical)	18 security updates are missing.
OURDS44	**Critical Updates, Office 2013**	**Failed (critical)**	**22 critical updates are missing.**
	Office 2013, Security Updates	Failed (non-critical)	19 security updates are missing.
	Security Updates, Windows Server 2012 R2	Failed (non-critical)	18 security updates are missing.

Missing Business-Class Endpoint Protection (Anti-virus)

35 PC’s & Servers



Computer Name	Anti-virus			Anti-spyware		
	Name	On	Current	Name	On	Curre
OUFILE2	None			None		
OUFILE4	None			None		
OUFO2	None			None		
OUGATE	None			None		
OUGMS3	None			None		
OUHQ	None			None		
OUMAIL	None			None		
OUPRINT2	None			None		

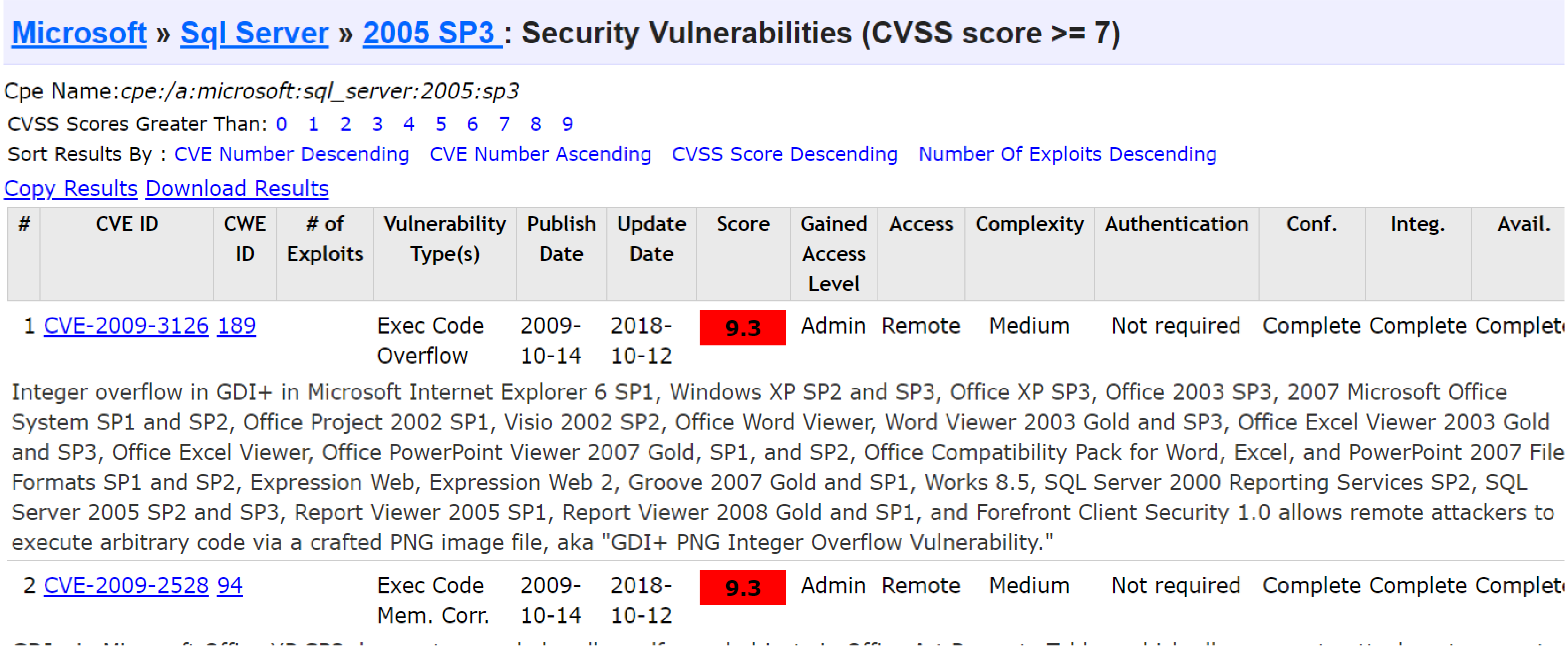
Unsupported Software (non-compliant with HIPAA)

SQL Server 2005 – 7 critical vulnerabilities
SQL Server 2008 – 2 critical vulnerabilities
Microsoft Server 2003 – 327 critical vulnerabilities
Crystal Reports 2008 – 1 critical vulnerability
Microsoft LiveMeeting 2007 – 18 critical vulnerabilities

Unsupported Software - SQL 2005

7 High Risks

Source: www.cvedetails.com



Microsoft » Sql Server » 2005 SP3 : Security Vulnerabilities (CVSS score >= 7)

Cpe Name:*cpe:/a:microsoft:sql_server:2005:sp3*

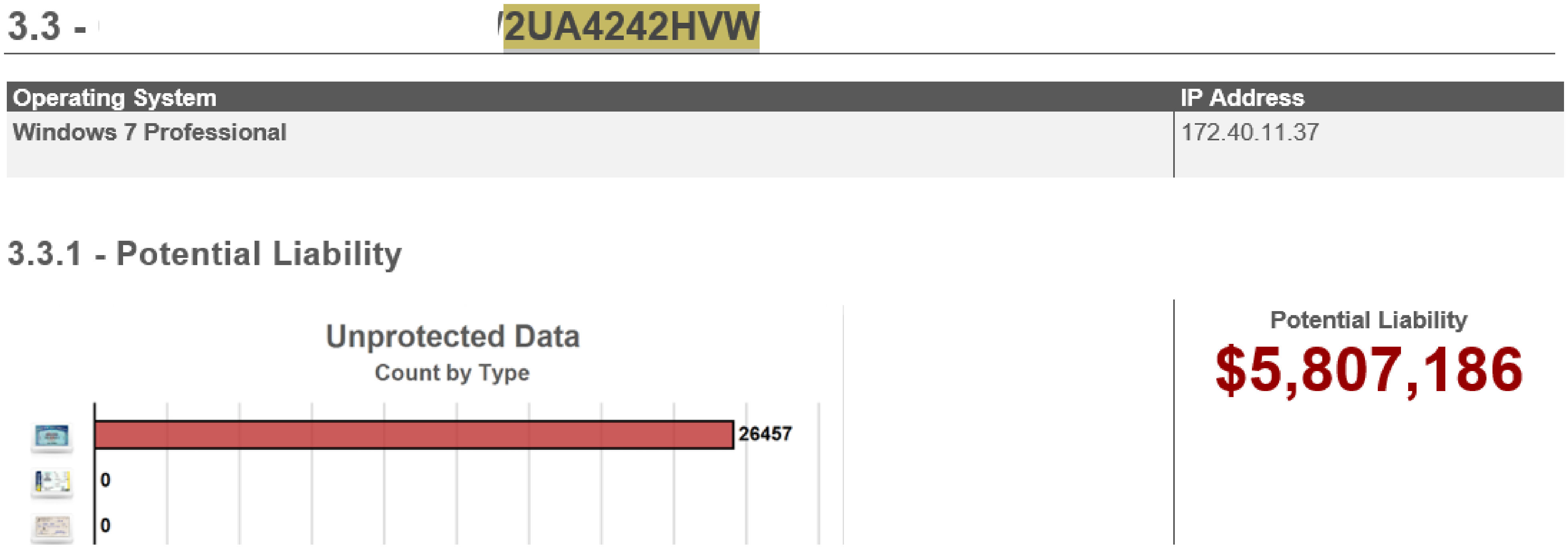
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2009-3126	189		Exec Code Overflow	2009-10-14	2018-10-12	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complet
Integer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Office Excel Viewer 2003 Gold and SP3, Office Excel Viewer, Office PowerPoint Viewer 2007 Gold, SP1, and SP2, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Expression Web, Expression Web 2, Groove 2007 Gold and SP1, Works 8.5, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2 and SP3, Report Viewer 2005 SP1, Report Viewer 2008 Gold and SP1, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a crafted PNG image file, aka "GDI+ PNG Integer Overflow Vulnerability."														
2	CVE-2009-2528	94		Exec Code Mem. Corr.	2009-10-14	2018-10-12	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complet

Social Security Numbers on Local PC



3.3 - [redacted] 2UA4242HVW

Operating System	IP Address
Windows 7 Professional	172.40.11.37

3.3.1 - Potential Liability

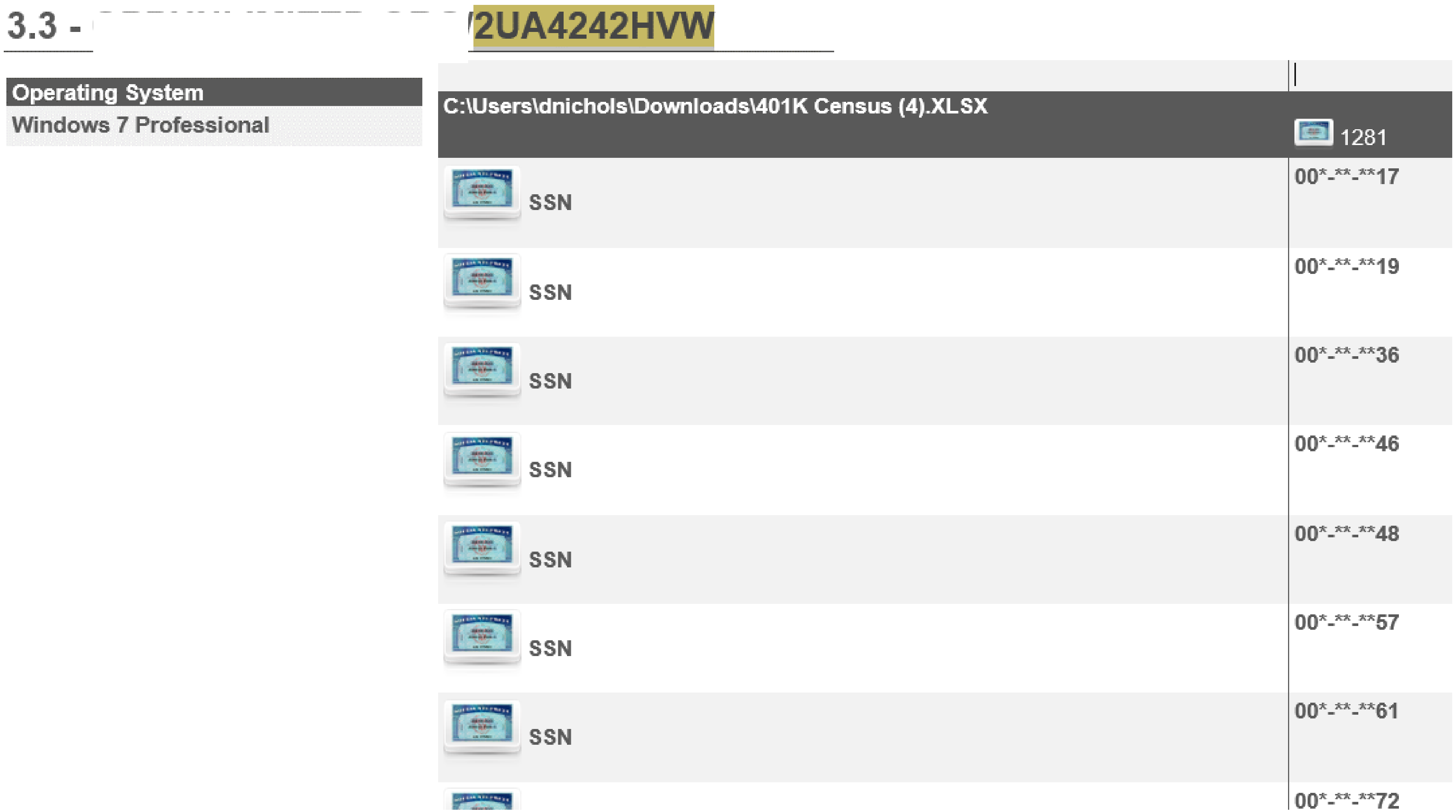
Unprotected Data

Count by Type

Potential Liability

$5,807,186

Social Security Numbers on Local PC



3.3 - [redacted]2UA4242HVW

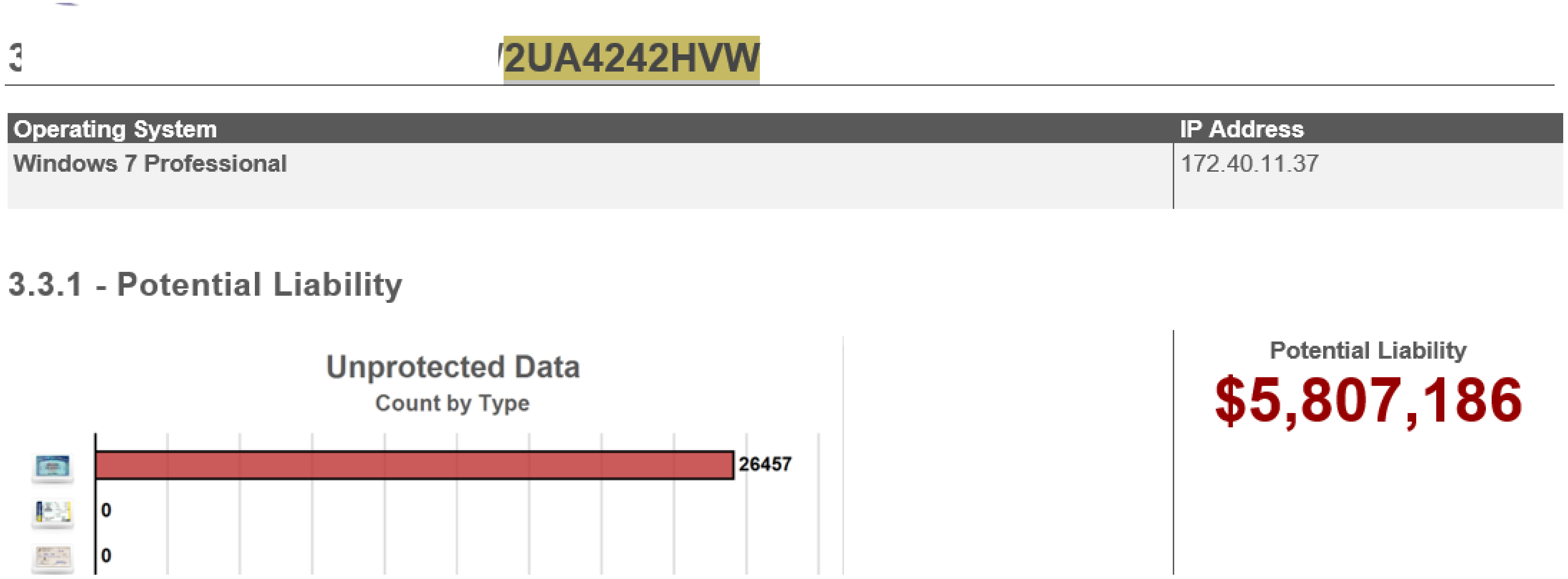
Operating System
Windows 7 Professional

C:\Users\dnichols\Downloads\401K Census (4).XLSX

1281

SSN	00*-**-**17
SSN	00*-**-**19
SSN	00*-**-**36
SSN	00*-**-**46
SSN	00*-**-**48
SSN	00*-**-**57
SSN	00*-**-**61
	00*-**-**72

Not Encrypted



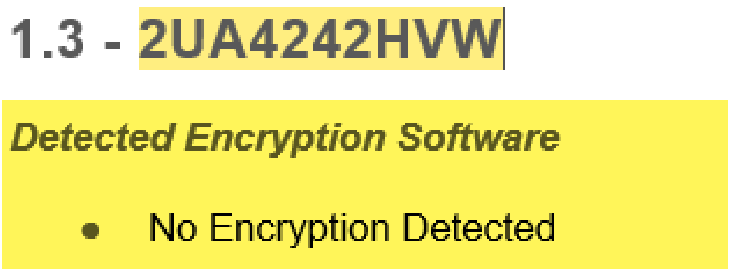
3 2UA4242HVW

Operating System	IP Address
Windows 7 Professional	172.40.11.37

3.3.1 - Potential Liability

Potential Liability

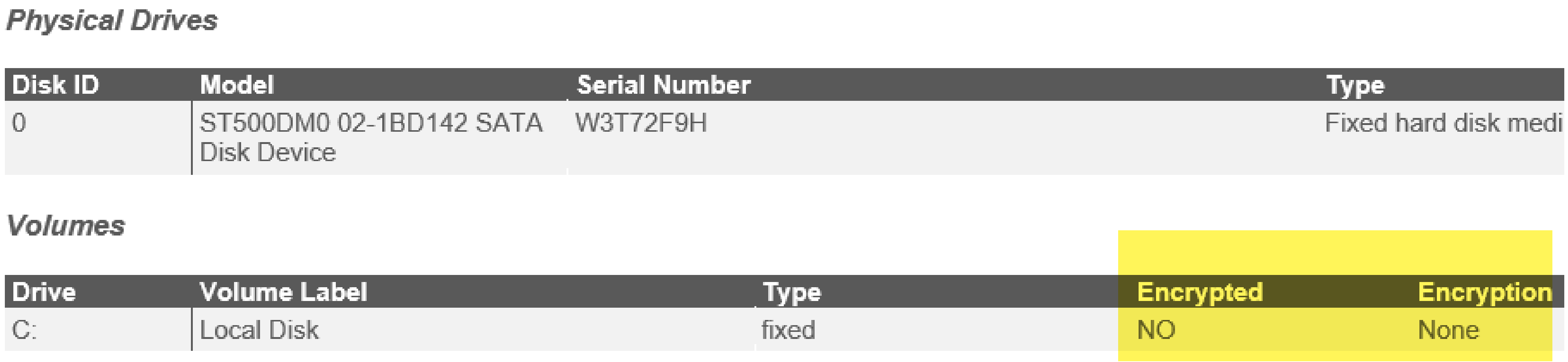
$5,807,186



1.3 - 2UA4242HVW

Detected Encryption Software

- No Encryption Detected



Physical Drives

Disk ID	Model	Serial Number	Type
0	ST500DM0 02-1BD142 SATA Disk Device	W3T72F9H	Fixed hard disk medi

Volumes

Drive	Volume Label	Type	Encrypted	Encryption
C:	Local Disk	fixed	NO	None

Policy Review

- **Encryption Policy** – All protected data must be encrypted.
- **Data Storage Policy** – Data must be saved to a server, not on a local workstation

NOT BEING FOLLOWED

HIPAA Penalties

2014 + 2015

$ 14 million

2016 + 2017

$ 42 million

2018 + 2019

$ 41 million

Key 2019 Penalties

- **URMC - $ 3 million**
  - Lost flash drive; personally-owned laptop with PHI stolen
- **Texas Health & Human Services Commission - $ 1.6 million**
  - No Audit Controls

Key 2019 Penalties

- **Touchstone Medical Imaging - $ 3 million**
  - Exposed Patient Data to the Internet
  - No Business Associate Agreement with IT Support vendor
  - No Business Associate Agreement with 3rd Party Data Center
  - No accurate or thorough Risk Analysis
  - Failed to Identify & Respond to IT incident
  - Failed to Notify Victims within time limit
  - Failed to Notify Media Outlets

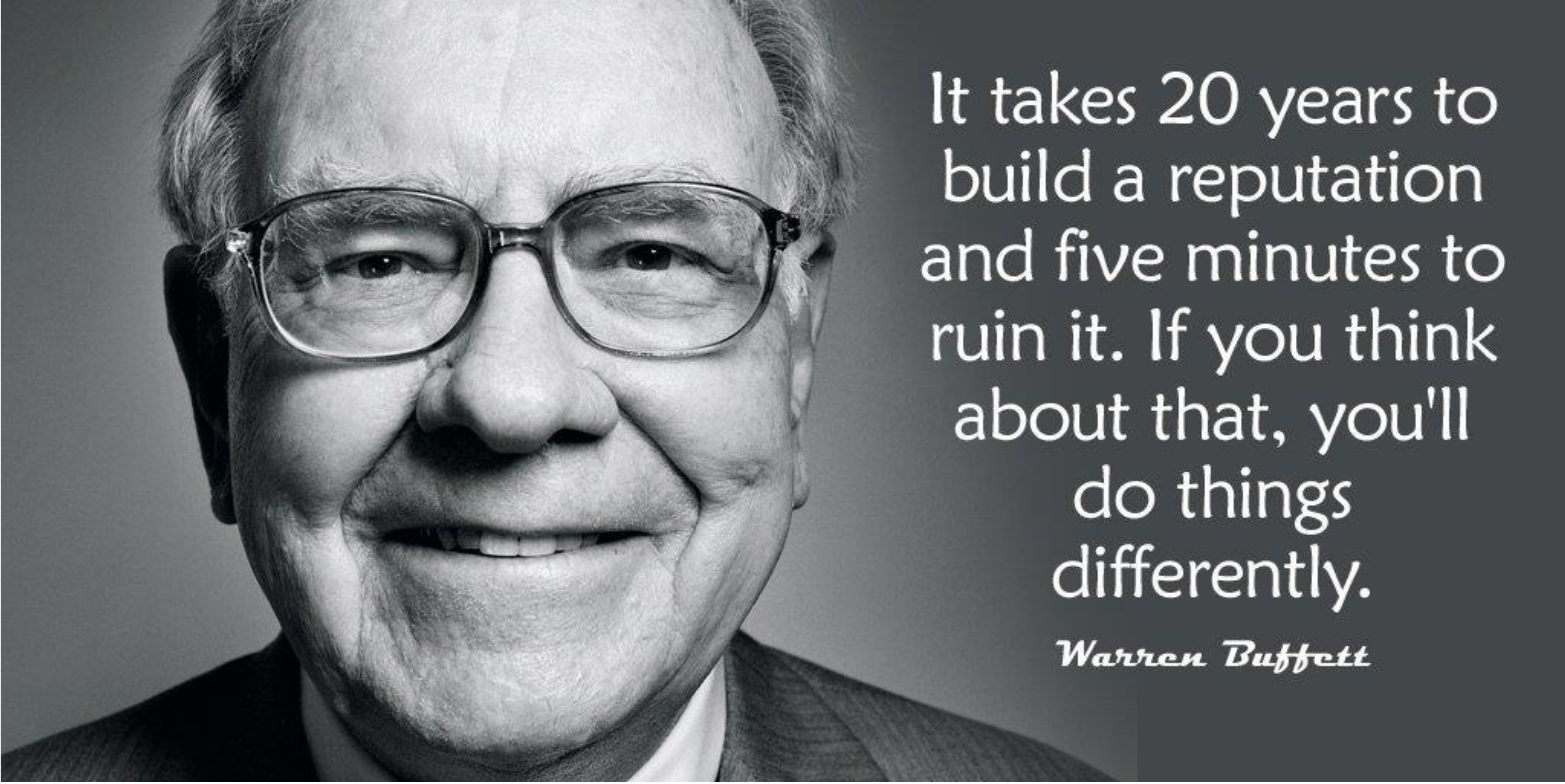
New York SHIELD Act Promises More Data Breach Enforcement, and International Reach

- **Stop Hacks and Improve Electronic Data Security** Act
  - Signed into law July 25, 2019
  - **Breach notification requirements went into effect October 23, 2019**
  - Data security requirements go into effect March 21, 2020
- **Applies to all businesses that store data about New Yorkers**
- **Expands definition of Private Information**
- **Changes breach to include 'access' to data instead of just 'acquiring' data**
  - *"indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."*
- **Requires reasonable data protection**
- **Failure considered an unfair business practice**

NY SHIELD Act - March 21, 2020 - Administrative, Technical, Physical Security Program

- 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

Data is Worth More Than Gold



It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.

Warren Buffett

QUESTIONS???

SEMEL CONSULTING

COMPLIANCE
CYBERSECURITY
BUSINESS CONTINUITY
PLANNING

ROSE KETCHUM
888-997-3635 X 202
rose@semelconsulting.com