NJHMR
HEALTHCARE MARKET REVIEW

BRACH EICHLER LLC

12TH ANNUAL **NJ HEALTHCARE MARKET REVIEW**

September 28-29, 2023

Borgata Hotel Casino & Spa Atlantic City, NJ

Security Breaches, Cyber Liability, and Effect on Sale Transactions

Lani M. Dornfeld, Esq., CHPC
Member
Brach Eichler LLC
Certified in Health Care Privacy Compliance
Moderator

Renee Bovelle, MD
Founder & CEO
Advanced Eyecare Medical Center
Master's in Cybersecurity

Neil A. Owens, CIC, Esq.
Managing Director
E.B. Cohen

Nelson Gomes
Executive Vice President of Business Development
Medicus IT

MODERATOR

Lani M. Dornfeld, Esq., CHPC

Member, Brach Eichler LLC

Lani M. Dornfeld is a Member in the Healthcare Practice Group. She is a seasoned healthcare and business attorney with a reputation for client responsiveness, attention to detail while not losing sight of the big picture, and providing sound legal guidance that takes into account the client's business needs and objectives. Her practice focuses on a wide variety of transactional, business, and regulatory matters, including sales and purchases of healthcare businesses, strategic partnerships, joint ventures, private equity investments and transactions, HIPAA compliance, corporate compliance, federal and state fraud and abuse laws, and contract negotiations. Lani also has deep experience in managing guardianship, patient care, informed consent, advance directive, and bioethical matters and issues.

Lani's clients include hospitals, health systems, management service organizations, surgery centers, substance use disorder treatment facilities, mental health treatment facilities, home health agencies, hospices, dental practices, medical practices, and individual healthcare providers.

A frequent lecturer and occasional adjunct professor, Lani is a sought-after speaker on a variety of health care topics. Lani also regularly contributes to Brach Eichler's monthly Health Law Update publication.

PANELISTS

Renee Bovelle, MD

Founder & CEO, Advanced Eyecare Medical Center

Renee Bovelle is the founder & CEO of Advanced Eyecare Medical Center, PA "dba" Envision Eye & Laser Center – currently serving over 20,000+ lives. She is a board-certified ophthalmologist, was trained at Wellesley College, UCLA School of Medicine, Yale University and the LSU Eye Center. She was pleased to be named a 2021 Washingtonian TOP DOCTOR by her peers. Additionally, Dr. Bovelle received a Master's in Cybersecurity Strategy and Information Management from GWU and focused on policies and practices that protect critical information with particular attention to the healthcare field. She has academic appointments at Howard University Hospital, Ross University School of Medicine, and the University of Maryland Capital Region Medical Center. She has been privileged to educate medical students, residents, and physicians locally and during national conferences on a broad array of issues in ophthalmology. Dr. Bovelle authored the first MedChi-approved continuing medical education course on Cybersecurity for Physicians and continues this work for both national and regional medical organizations. Additionally, she authored a chapter in *"Navigating A Triple Pandemic: Volume 3: Claiming Our Healing & Embracing a New Normal".*

PANELISTS

Neil A. Owens, CIC, Esq.

Managing Director, E.B. Cohen

As Managing Director at E.B. Cohen, A Hilb Group Company, Neil manages the Roseland, NJ office. Neil develops long term client relationships by applying his unique expertise to client needs. With over 24 years of experience, Neil delivers caring, professional solutions to complex insurance and risk management problems.

Neil earned his Bachelor of Business Administration from the College of William and Mary in Williamsburg, Virginia in 1999. In 2000, he earned his Certified Insurance Counselor (CIC) designation. At the time, he had the distinction of being the youngest person to earn a CIC. A lifelong learner, he went on to obtain his J.D. from Seton Hall University Law School in 2005 and became a member of the New Jersey Bar Association. He frequently provides educational workshops on various aspects of commercial insurance and cyber insurance. In 2018 Neil spoke at the prestigious William & Mary Mason School of Business event Cybersecurity Conference of Experts.

EB Cohen has been an industry leader specializing in all areas of Insurance & Risk Management for the healthcare industry. EB Cohen is A Hilb Group Company with over 130 offices across the country. As a top 20 agency, The Hilb Group affords clients the comfort that their insurance is with a premiere, best in class organization.

PANELISTS

Nelson Gomes,

Senior Vice President of Business Development, Medicus IT

Nelson Gomes is an accomplished healthcare IT executive with over 25 years of experience in the industry. He passionately advocates for leveraging technology to enhance patient care while transforming the business of healthcare. Currently, Nelson serves as the Executive Vice President of Business Development at Medicus IT, where he spearheads business growth and development initiatives.

Nelson's journey in healthcare IT began with the founding of PriorityOne Group in 1997, a premier provider of healthcare IT services and solutions. Under his leadership, PriorityOne Group grew to become a recognized leader in the industry, pioneering innovative solutions that enabled healthcare organizations to utilize technology for improving patient care, optimizing operations, and managing costs.

In his current role at Medicus IT, Nelson is dedicated to helping healthcare organizations navigate the complex landscape of healthcare IT and to delivering innovative solutions that drive business growth and improve patient care. Nelson is passionate about cultivating strong business relationships with clients, partners, and healthcare industry leaders and values the opportunity to collaborate with the exceptional team at Medicus IT. His contributions reflect a deep-seated drive to revolutionize the healthcare landscape through the strategic use of technology.

Security Breaches, Cyber Liability, and effect on Sale Transactions:

Security Breaches are Real and Costing Healthcare Businesses Millions. What to Do?

The Top 5

Cyber Threats Facing the Health and Public Health Sector & Cybersecurity Best Practices

- **Social Engineering**
  - attempt to trick you into giving out personal information or infecting your device by clicking on a link to give hackers access to patient data
- **Ransomware**
  - an attack that occurs when hackers gain control of data or a computer system and hold it hostage until a ransom is paid
- **Loss or Theft of Equipment or Data**
  - loss or theft of devices such as laptops, smart phones and devices, USB/thumb drives, etc. that could get into the hands of hackers
- **Insider, Accidental or Malicious Data Loss**
  - negligent or deliberate acts by employees, former employees, contractors, etc.
- **Attacks Against Network Connected Devices**
  - e.g., file server attached to a medical device, devices with hard drives, devices that communicate from remote locations, etc.

https://405d.hhs.gov/Documents/HICP-Main-508.pdf

Implementation of cybersecurity best practices

Costs of a Data Breach

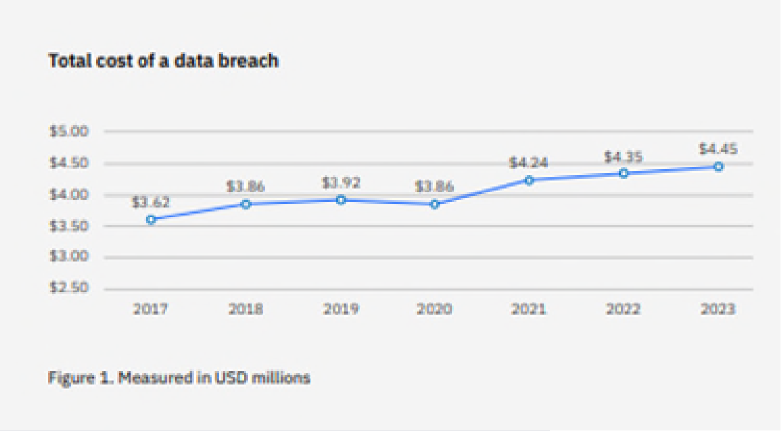

Total cost of a data breach

Figure 1. Measured in USD millions

"A healthcare data breach is among the costliest types of data breach. The average cost of a data breach across industries [from March 2022 to March 2023] was $4.45 million, yet the average cost of a healthcare data breach was the highest among all industries at $10.93 million. Healthcare has seen a significant cost increase of 53.3% over the past three years."

https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/

Costs can include:

- Forensic investigation and response
- Other experts, including legal
- Lost business
- Consumption of human resources
- Notification expenses
- Implementation of corrective measures
- Fines and penalties
- Lawsuits

Bottom Line: Breach events affect the bottom line.

Health Care Transactions

Breaches and Lack of Best Pratices

- Current buyer landscape is sophisticated, and buyers typically will do a deep dive into due diligence, including regulatory compliance across the board
  - this includes data privacy and security compliance

- Due diligence can reveal:
  - Lack of privacy and security officer positions with real functions
  - Lack of/outdated policies and procedures
  - Lack of or lax training initiatives
  - Failure to perform periodic security risk assessments
  - Failure to develop and implement a risk management plan in response to risk assessments or identified weaknesses or vulnerabilities
  - Poor or weak IT systems and oversight
  - Past or present privacy or security breach events

- Diligence findings may result in:
  - Reduced purchase price
  - Larger than normal indemnification escrows in sale contract
  - Special indemnification provisions in sale contract
  - Indemnification claims post-closing

Why Should I Care About Cybersecurity?

Healthcare is a Prime Target for Nation-States and Cyber Criminals

Protected Health Information

Blackmail

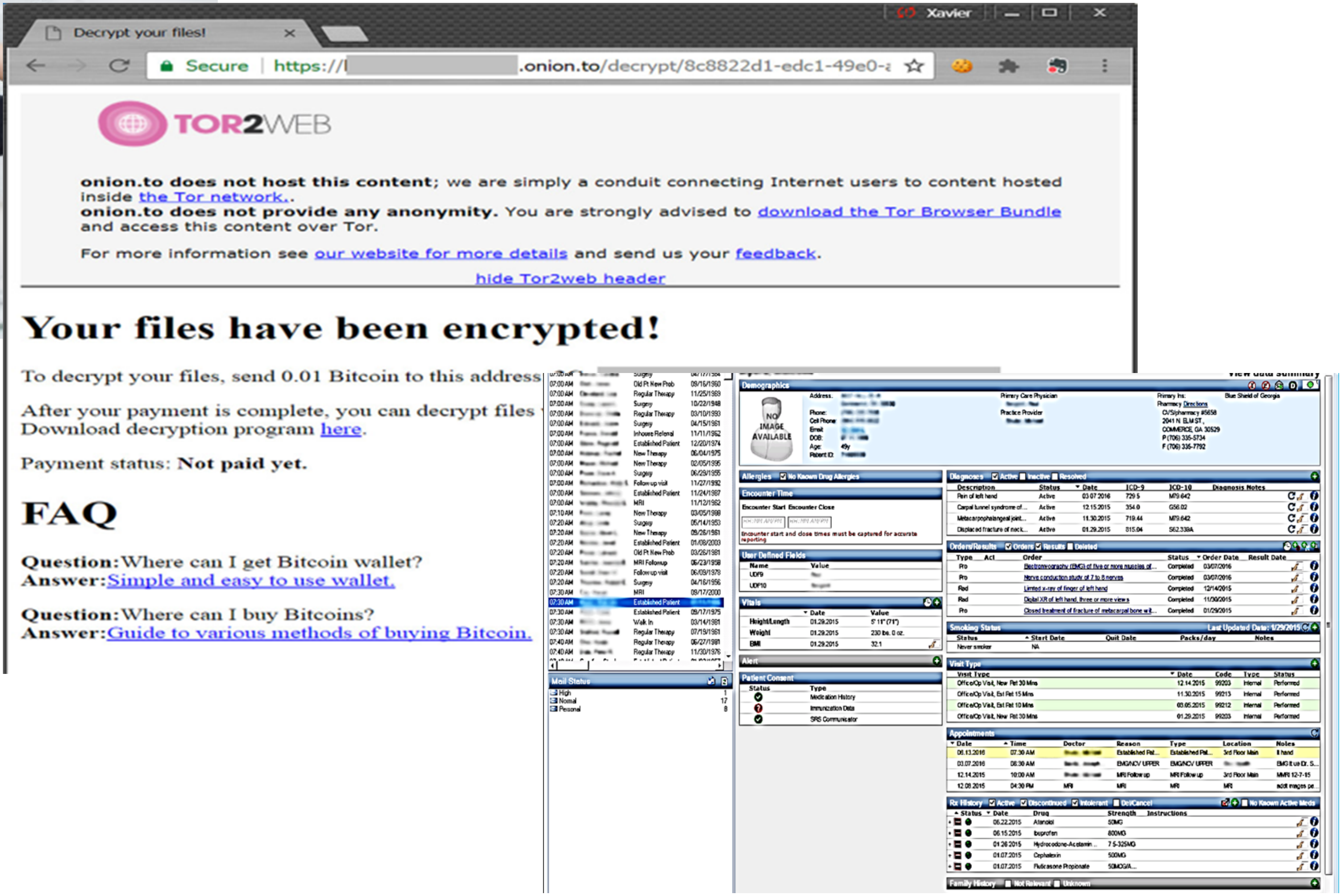
Espionage

Extortion

Intellectual Property

Payment Card Information

Healthcare is a Prime Target for Nation-States and Cyber Criminals



TOR2WEB

onion.to does not host this content; we are simply a conduit connecting Internet users to content hosted inside the Tor network..
onion.to does not provide any anonymity. You are strongly advised to download the Tor Browser Bundle and access this content over Tor.

For more information see our website for more details and send us your feedback.

hide Tor2web header

Your files have been encrypted!

To decrypt your files, send 0.01 Bitcoin to this address

After your payment is complete, you can decrypt files
Download decryption program here.

Payment status: **Not paid yet.**

FAQ

Question: Where can I get Bitcoin wallet?
Answer: Simple and easy to use wallet.

Question: Where can I buy Bitcoins?
Answer: Guide to various methods of buying Bitcoin.

07:00 AM	[redacted]	Old Pt New Prob	09/16/1960
07:00 AM	[redacted]	Regular Therapy	11/25/1969
07:00 AM	[redacted]	Surgery	10/22/1948
07:00 AM	[redacted]	Regular Therapy	03/10/1993
07:00 AM	[redacted]	Surgery	04/15/1961
07:00 AM	[redacted]	Inhouse Referral	11/11/1962
07:00 AM	[redacted]	Established Patient	12/20/1974
07:00 AM	[redacted]	New Therapy	06/04/1975
07:00 AM	[redacted]	New Therapy	02/05/1995
07:00 AM	[redacted]	Surgery	06/29/1955
07:00 AM	[redacted]	Follow up visit	11/27/1992
07:00 AM	[redacted]	Established Patient	11/24/1987
07:00 AM	[redacted]	MRI	11/12/1962
07:10 AM	[redacted]	New Therapy	03/05/1998
07:20 AM	[redacted]	Surgery	05/14/1953
07:20 AM	[redacted]	New Therapy	09/26/1961
07:20 AM	[redacted]	Established Patient	01/08/2003
07:20 AM	[redacted]	Old Pt New Prob	03/26/1981
07:20 AM	[redacted]	MRI Followup	06/23/1958
07:20 AM	[redacted]	Follow up visit	06/09/1978
07:20 AM	[redacted]	Surgery	04/16/1956
07:30 AM	[redacted]	MRI	09/17/2000
07:30 AM	[redacted]	Established Patient	[redacted]
07:30 AM	[redacted]	Established Patient	09/17/1975
07:30 AM	[redacted]	Walk In	03/14/1981
07:30 AM	[redacted]	Regular Therapy	07/19/1961
07:40 AM	[redacted]	Regular Therapy	06/27/1981
07:40 AM	[redacted]	Regular Therapy	11/30/1976

Mail Status

High	1
Normal	17
Personal	8

View Data Summary

Demographics

NO IMAGE AVAILABLE

Address: [redacted]
Phone: [redacted]
Cell Phone: [redacted]
Email: [redacted]
DOB: [redacted]
Age: 49y
Patient ID: [redacted]

Primary Care Physician [redacted]
Practice Provider [redacted]

Primary Ins: Blue Shield of Georgia
Pharmacy Directions
CVS/pharmacy #5658
2041 N. ELM ST.,
COMMERCE, GA 30529
P (706) 335-5734
F (706) 335-7792

Allergies ☑ No Known Drug Allergies

Encounter Time

Encounter Start Encounter Close

HH:MM AM/PM HH:MM AM/PM

Encounter start and close times must be captured for accurate reporting

User Defined Fields

Name	Value
UDF9	[redacted]
UDF10	[redacted]

Vitals

	Date	Value
Height/Length	01.29.2015	5' 11" (71")
Weight	01.29.2015	230 lbs. 0 oz.
BMI	01.29.2015	32.1

Alert

Patient Consent

Status	Type
✓	Medication History
?	Immunization Data
✓	SRS Communicator

Diagnoses ☑ Active ☐ Inactive ☐ Resolved

Description	Status	Date	ICD-9	ICD-10	Diagnosis Notes
Pain of left hand	Active	03.07.2016	729.5	M79.642	
Carpal tunnel syndrome of...	Active	12.15.2015	354.0	G56.02	
Metacarpophalangeal joint...	Active	11.30.2015	719.44	M79.642	
Displaced fracture of neck...	Active	01.29.2015	815.04	S62.338A	

Orders/Results ☑ Orders ☑ Results ☐ Deleted

Type	Act	Order	Status	Order Date	Result Date
Pro		Electromyography (EMG) of five or more muscles of...	Completed	03/07/2016	
Pro		Nerve conduction study of 7 to 8 nerves	Completed	03/07/2016	
Rad		Limited x-ray of finger of left hand	Completed	12/14/2015	
Rad		Digital XR of left hand, three or more views	Completed	11/30/2015	
Pro		Closed treatment of fracture of metacarpal bone wit...	Completed	01/29/2015	

Smoking Status Last Updated Date: 1/29/2015

Status	Start Date	Quit Date	Packs/day	Notes
Never smoker	NA			

Visit Type

Visit Type	Date	Code	Type	Status
Office/Op Visit, New Pat 30 Mins	12.14.2015	99203	Internal	Performed
Office/Op Visit, Est Pat 15 Mins	11.30.2015	99213	Internal	Performed
Office/Op Visit, Est Pat 10 Mins	03.05.2015	99212	Internal	Performed
Office/Op Visit, New Pat 30 Mins	01.29.2015	99203	Internal	Performed

Appointments

Date	Time	Doctor	Reason	Type	Location	Notes
06.13.2016	07:30 AM	[redacted]	Established Pat...	Established Pat...	3rd Floor Main	lt hand
03.07.2016	08:30 AM	[redacted]	EMG/NCV UPPER	EMG/NCV UPPER	[redacted]	EMG lt ue Dr. S...
12.14.2015	10:00 AM	[redacted]	MRI Follow up	MRI Follow up	3rd Floor Main	MMRI 12-7-15
12.08.2015	04:30 PM	MRI	MRI	MRI	MRI	addl images pe...

Rx History ☑ Active ☑ Discontinued ☑ Intolerant ☐ Del/Cancel ☐ No Known Active Meds

Status	Date	Drug	Strength	Instructions
●	06.22.2015	Atenolol	50MG	
●	06.15.2015	Ibuprofen	800MG	
●	01.26.2015	Hydrocodone-Acetamin...	7.5-325MG	
●	01.07.2015	Cephalexin	500MG	
●	01.07.2015	Fluticasone Propionate	50MCG/A...	

Family History ☐ Not Relevant ☐ Unknown

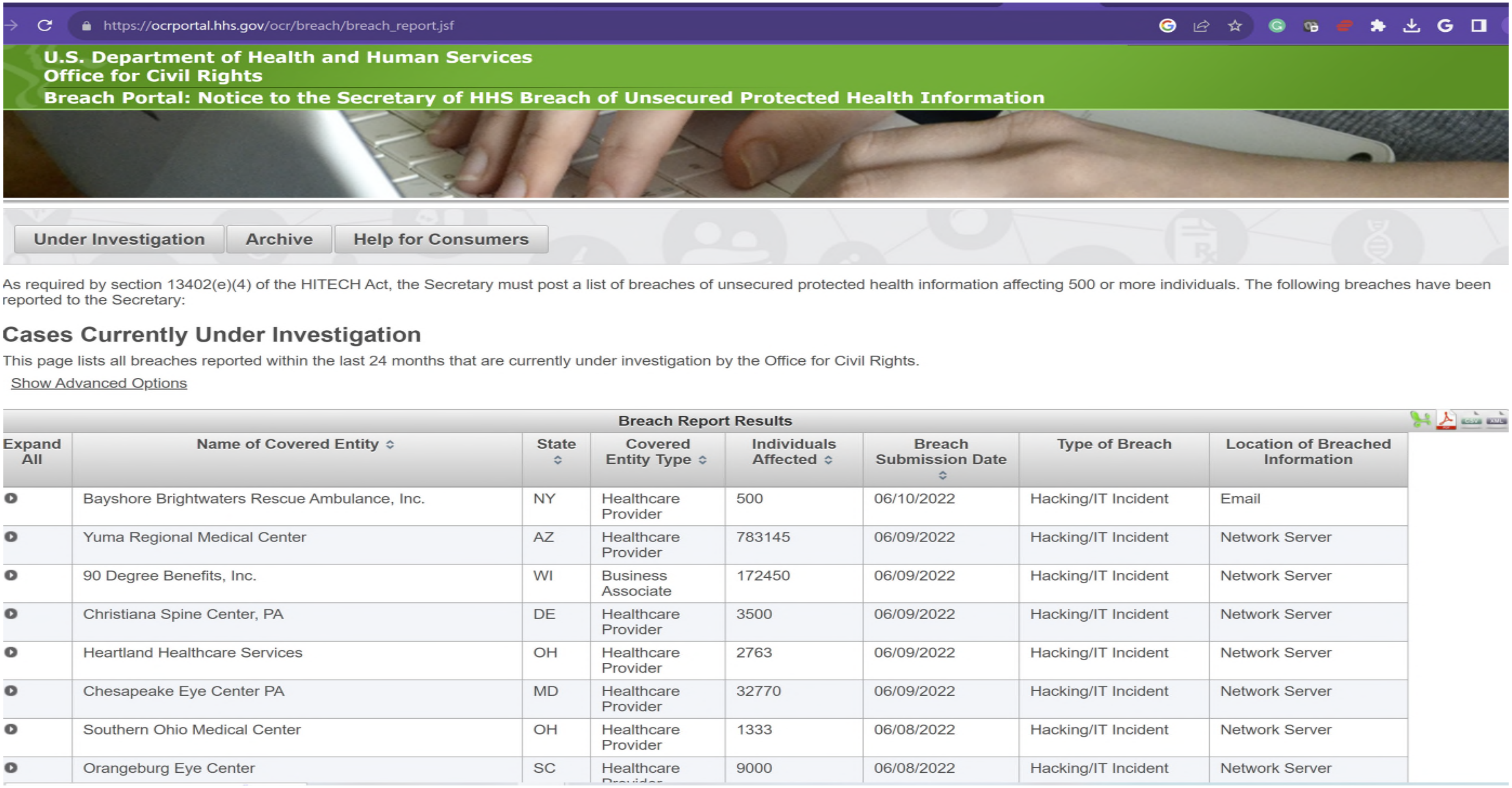
Put on the DarkWeb by the Dark Overlord

Doe, D. (2017, March 24). 655,000 patient records for sale on the dark net after hacking victims refuse extortion demands. The Daily Dot

RELEVANCE

- Healthcare data breach costs you on average $499+/record 2021 (Bitglass HealthcareBreachReport2021)
- Average healthcare breach in US 10.93 million (IBM 2023 data breach report)
- 83% of physicians had cyber attack (2017 AMA/ Accenture Survey)
- 99.9 % of web application penetration tests result in access to ePHI (2018 Horizon Report: THE STATE OF CYBERSECURITY IN HEALTHCARE)
- Health records of about 42 Million Americans breached btwn 2016 -2021 (Jama Health Forum 2022)
- 95% of identity theft comes from stolen healthcare records *(Source: Globe NewsWire)*
- Feds warn of 'exceptionally aggressive' ransomware threat targeting healthcare (Fierce Health care Apr 21, 2022)

Wall of Shame



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	Bayshore Brightwaters Rescue Ambulance, Inc.	NY	Healthcare Provider	500	06/10/2022	Hacking/IT Incident	Email
●	Yuma Regional Medical Center	AZ	Healthcare Provider	783145	06/09/2022	Hacking/IT Incident	Network Server
●	90 Degree Benefits, Inc.	WI	Business Associate	172450	06/09/2022	Hacking/IT Incident	Network Server
●	Christiana Spine Center, PA	DE	Healthcare Provider	3500	06/09/2022	Hacking/IT Incident	Network Server
●	Heartland Healthcare Services	OH	Healthcare Provider	2763	06/09/2022	Hacking/IT Incident	Network Server
●	Chesapeake Eye Center PA	MD	Healthcare Provider	32770	06/09/2022	Hacking/IT Incident	Network Server
●	Southern Ohio Medical Center	OH	Healthcare Provider	1333	06/08/2022	Hacking/IT Incident	Network Server
●	Orangeburg Eye Center	SC	Healthcare Provider	9000	06/08/2022	Hacking/IT Incident	Network Server

1st 6month 2023 HHS Healthcare Breach Data

Researchers at Critical Insight

- Victims of healthcare data breaches climbed to 40 million
- 73% were due to hacking or IT incidents
- 21% of hacking breaches were targeted at ***business associates***
- 14% at health plans
- Remainder at ***individual healthcare providers***

THE DATA

Research Suggests Healthcare Data Breaches Cause 2,100 Deaths a Year

Vanderbilt University conducted a study that suggests mortality rates at hospitals rise after a data breach.

Sung Choi, PhD 2018

Choi notes that after a breached hospitals mortality rates increase after a data breach HIPAA covered entities must develop contingency plans for emergencies such as cyberattacks and ransomware incidents.

Source: https://www.hipaajournal.com/research-suggests-healthcare-data-breaches-cause-2100-deaths-a-year/

THE DATA

Ransomware Attack Shuts down Michigan Practice – Deletes All Patient Files

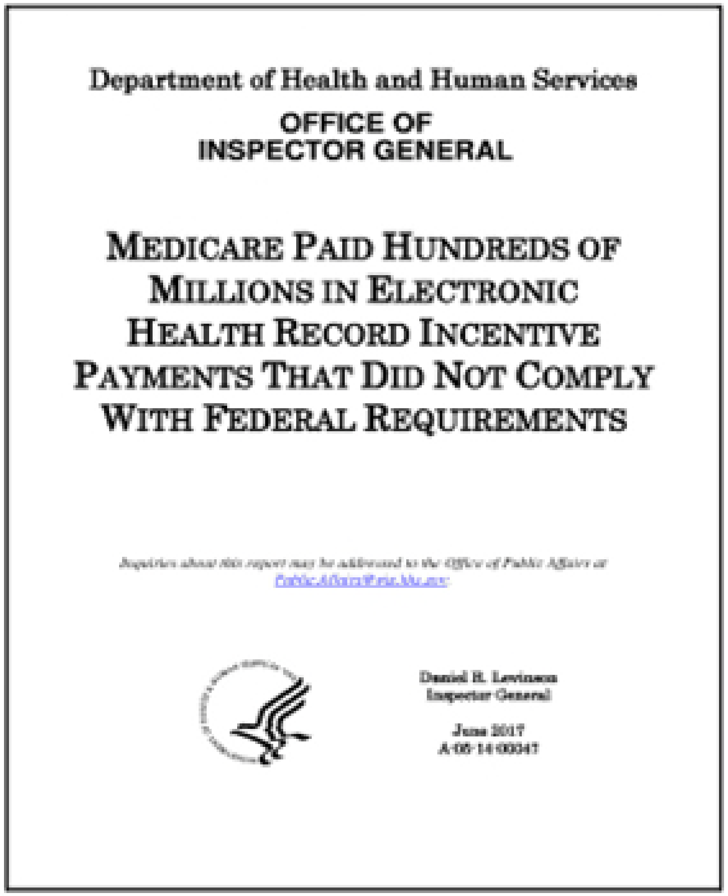
Posted in: HITECHAnswers.net
By: Art Gross 20 May 2019

'Health care is not prepared': Physician details deficiencies in market's ability to combat Ransomware threats

July 20, 2021

PATIENTS LEFT WITH NO MEDICAL RECORDS FOLLOWING RANSOMWARE ATTACK ON MICHIGAN PRACTICE

CMS Begins First-Ever MIPS Audits, Covers 2017 & 2018 Reporting



Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

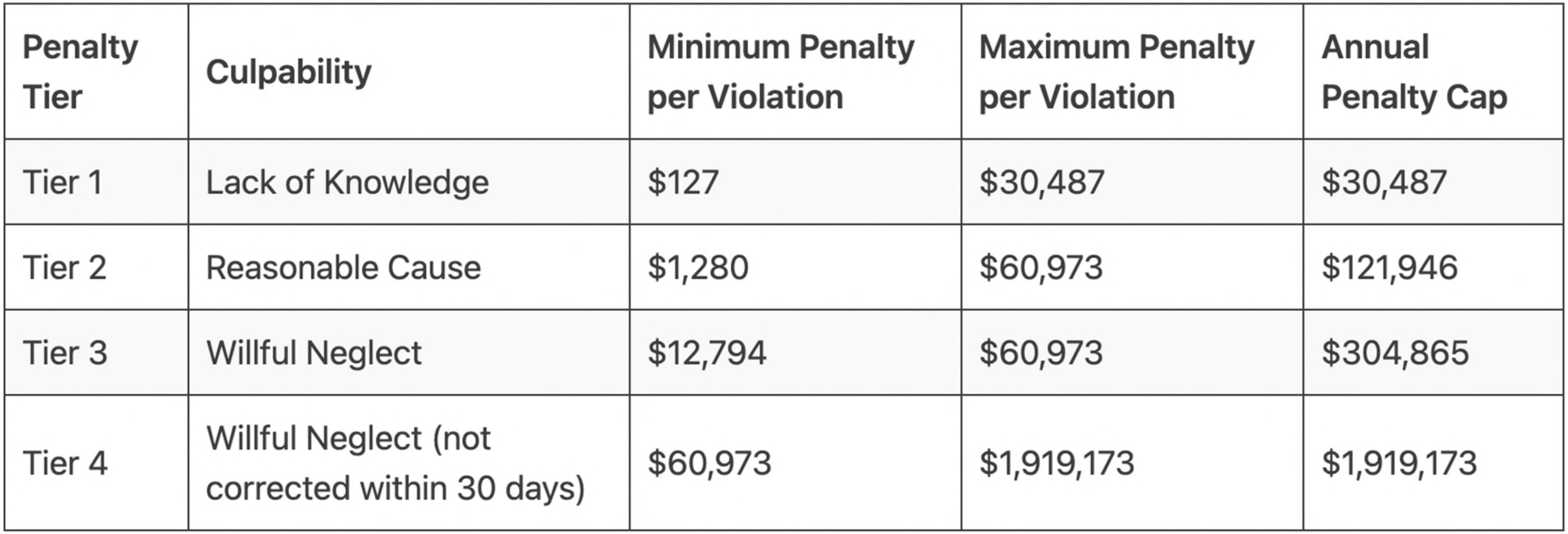
Medicare Paid Hundreds of Millions in Electronic Health Record Incentive Payments That Did Not Comply With Federal Requirements

Inquiries about this report may be addressed to the Office of Public Affairs at
Public.Affairs@oig.hhs.gov.

Daniel R. Levinson
Inspector General

June 2017
A-05-14-00047

HIPAA PENALTIES 2023



Penalty Tier	Culpability	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of Knowledge	$127	$30,487	$30,487
Tier 2	Reasonable Cause	$1,280	$60,973	$121,946
Tier 3	Willful Neglect	$12,794	$60,973	$304,865
Tier 4	Willful Neglect (not corrected within 30 days)	$60,973	$1,919,173	$1,919,173

Business Associate Agreements (BAAs)

- The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity
- Outline how PHI will be handled between the covered entity and the business associate and who is responsible should a breach occur.
- In OCR investigations where BAAs were not properly executed, Covered Entities that had nothing to do with the breach that incited the investigation were held liable for the loss of data.
- BAAs mandated by federal regulation / best interest of protecting your organization's reputation.

Examples of BAAs

- 1099 employees
- Accrediting bodies
- Answering services/messaging services
- Consultants
- Delivery companies
- EHR/EMR companies/consultants
- Hosting servers
- IT companies
- Medical billing/coding companies/consultants
- Mobile apps and texting services
- Patient safety organizations
- Staffing agencies
- Wholesalers

- Shredding/Mobile Shredding Services
- Answering Services
- Clearing Houses
- Software as a Service (SaaS)
- Telehealth
- Telemental Health
- Marketing Companies
- Print and Mailing Services
- Transportation Services
- Managed Service providers (MSP’s)
- Website development companies
- Point of sale systems
- Practice management software
- Nursing homes, personal care homes, adult communities, assisted living communities

Benefits Of Digital Forensics

DETERMINE LIABILITY

PROTECT ASSETS

SECURE DEVICES

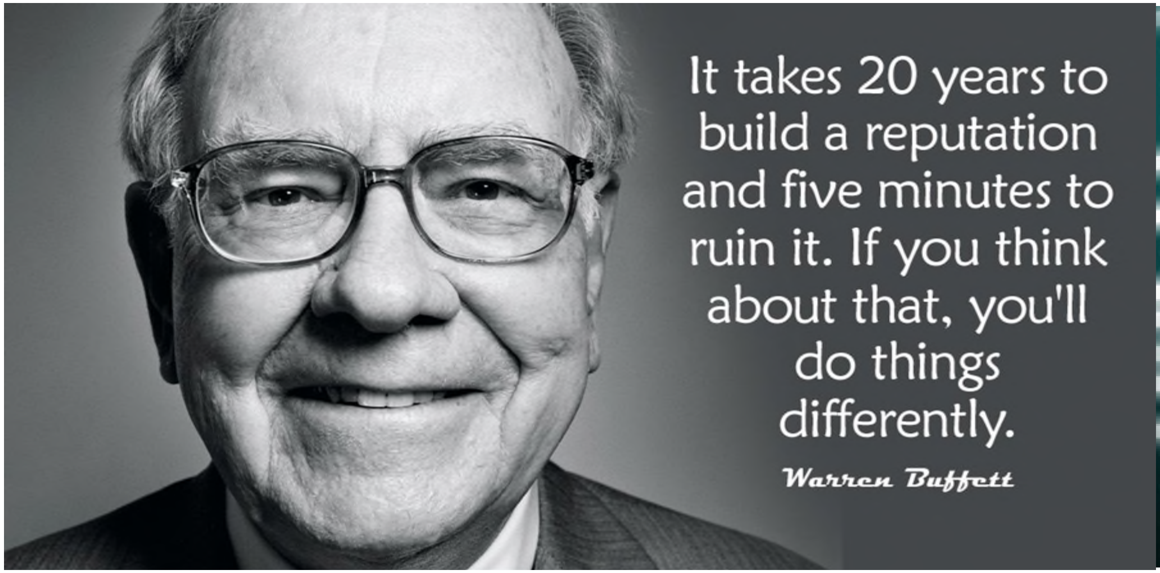
RECOVER LOST INFORMATION

LOCATE DATA

ACCESS & DECRYPT PROTECTED / HIDDEN FILES

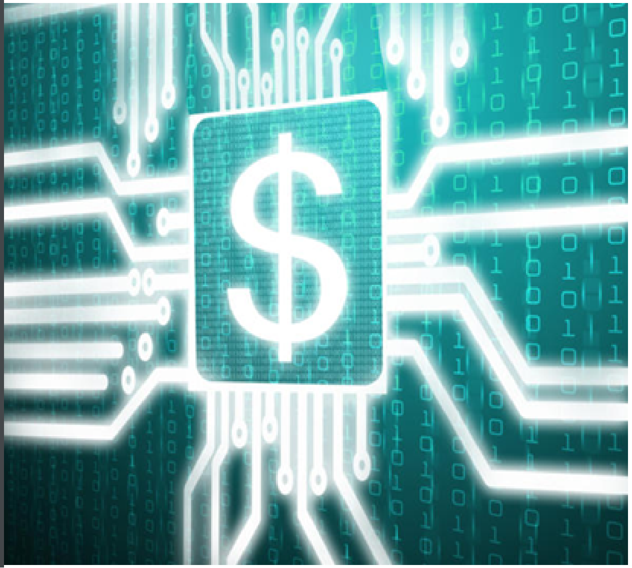
DOCUMENTATION FOR AUTHORITIES / COURT

Invest Now or Pay MORE Later $$



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

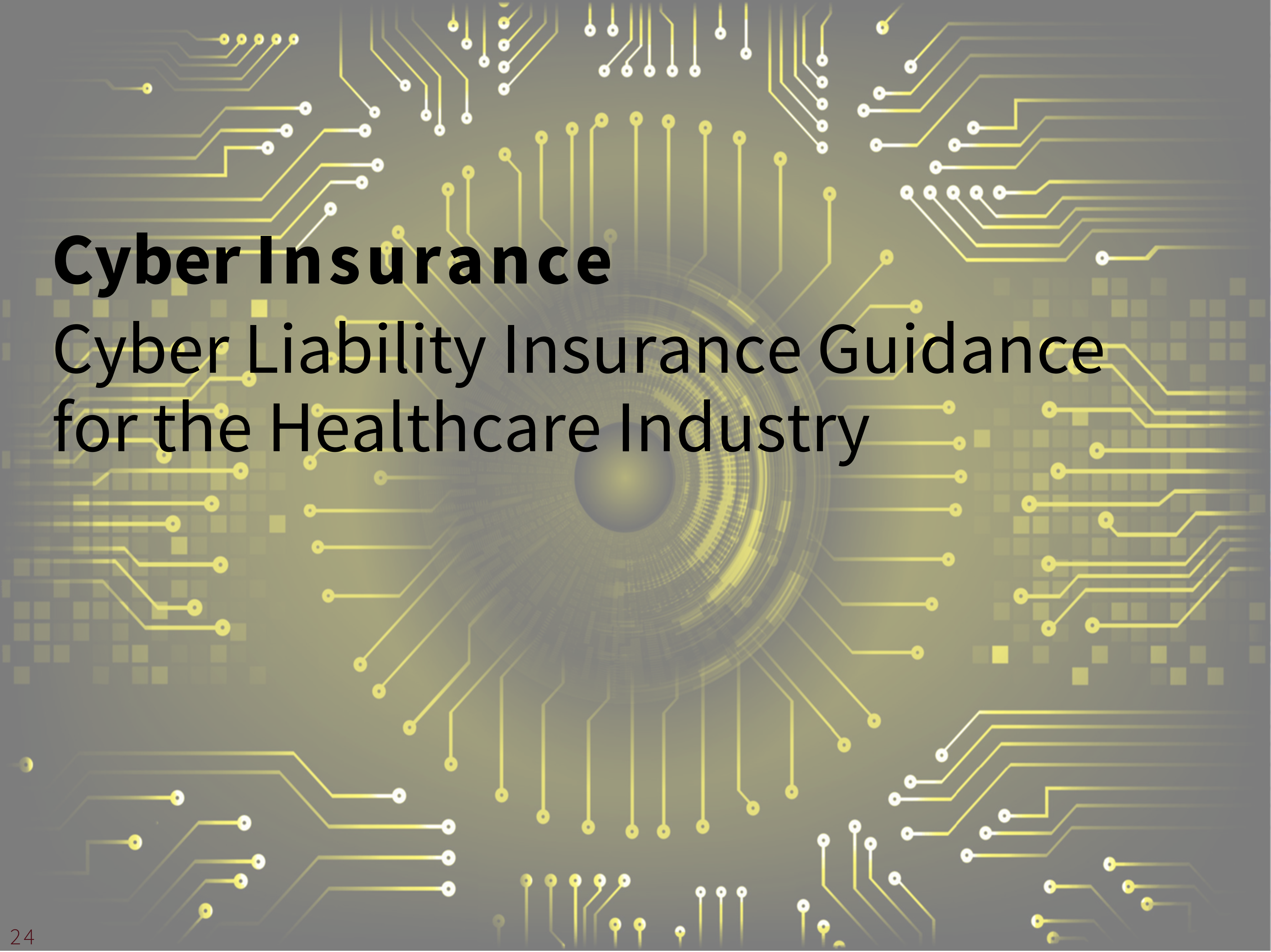


$$$ Invest Now or Pay MORE Later $$$
Alarming state of cybersecurity in healthcare facilities

Allocate cybersecurity $$ to Budget
EDUCATE STAFF & LEAD BY EXAMPLE

Policy / Procedures and Security Risk Assessment

New Employees and Annual Training



Cyber Insurance

Cyber Liability Insurance Guidance for the Healthcare Industry

slido

What is the gross revenue of your organization?

ⓘ Start presenting to display the poll results on this slide.

Coverage Components Available In Cyber Insurance Marketplace Today

- **1st Party Coverage:** 1. Privacy Event Crisis Management Expense & Notification expense coverage. 2. Business Interruption & Extra Expense. 3. Data Assets. 4. Cyber Extortion. 5. Computer Fraud. 6. Funds Transfer Fraud. 7. Social Engineering Coverage.

- **3rd Party Coverage:** 1. Information Security and Privacy Liability. 2. Regulatory Defense and Penalty. 3. Payment Card Industry Fines and Assessments. 4 Website Media. 5. Bodily Injury & Property Damage

How Does a Cyber Policy Work?

- Immediate Access to Data Breach Coach – an attorney – that offers guidance, arranges needed breach management resources and maintains privilege. Tip: Consider your data breach coach relationship prior to a breach. Do you have counsel you prefer? Make certain they are approved on your insurance policy at the time the coverage is placed, not after a breach. Arrange this with your trusted insurance broker.

- 1st party expenses related to a forensic investigation of the breach itself. Notification expenses, legals expenses, etc.
- 3rd party liabilities are defended and/or settled.

What Does it Accomplish?

- The Cyber policy limits can absorb the **financial impact** of a breach.
- The Cyber policy affords ease of **access** to industry leading experts to manage a breach crisis and maintain the reputation of your organization.
- The Cyber policy provides **pro-active risk management guidance** and breach awareness training services.
- A cyber policy affords peace of mind for risks that are difficult to prevent, prepare for, and manage.

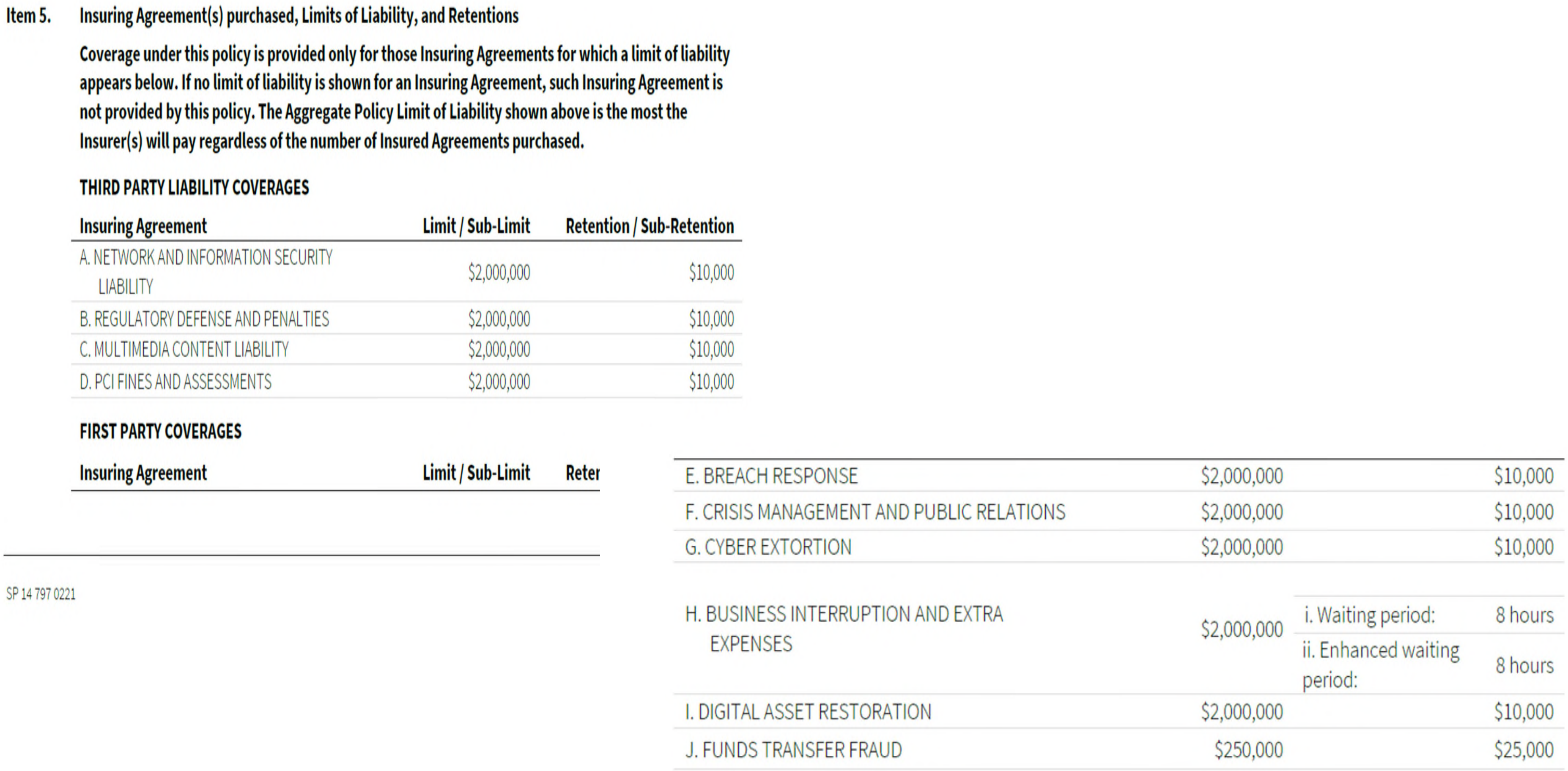
Cyber Included on Malpractice?

- The Cyber coverage that may be included on your malpractice is NOT sufficient to protect your organization!

- In general malpractice insurance companies would prefer to include some token coverage and pay some low level of claim to avoid litigation about whether the primary coverage parts include Cyber. By offering a rider (aka endorsement) that includes limited coverage, a malpractice carrier avoids coverage litigation.

- It is advisable to obtain a separate Cyber Insurance Program with both 1st party coverage AND 3rd party coverage.

Sample Coverage to Compare



Item 5. **Insuring Agreement(s) purchased, Limits of Liability, and Retentions**

Coverage under this policy is provided only for those Insuring Agreements for which a limit of liability appears below. If no limit of liability is shown for an Insuring Agreement, such Insuring Agreement is not provided by this policy. The Aggregate Policy Limit of Liability shown above is the most the Insurer(s) will pay regardless of the number of Insured Agreements purchased.

THIRD PARTY LIABILITY COVERAGES

Insuring Agreement	Limit / Sub-Limit	Retention / Sub-Retention
A. NETWORK AND INFORMATION SECURITY LIABILITY	$2,000,000	$10,000
B. REGULATORY DEFENSE AND PENALTIES	$2,000,000	$10,000
C. MULTIMEDIA CONTENT LIABILITY	$2,000,000	$10,000
D. PCI FINES AND ASSESSMENTS	$2,000,000	$10,000

FIRST PARTY COVERAGES

Insuring Agreement	Limit / Sub-Limit	Reter
E. BREACH RESPONSE	$2,000,000	$10,000
F. CRISIS MANAGEMENT AND PUBLIC RELATIONS	$2,000,000	$10,000
G. CYBER EXTORTION	$2,000,000	$10,000
H. BUSINESS INTERRUPTION AND EXTRA EXPENSES	$2,000,000	i. Waiting period: 8 hours ii. Enhanced waiting period: 8 hours
I. DIGITAL ASSET RESTORATION	$2,000,000	$10,000
J. FUNDS TRANSFER FRAUD	$250,000	$25,000

SP 14 797 0221

Market Leaders Today

Coalition™

beazley

CHUBB

TRAVELERS

AXIS

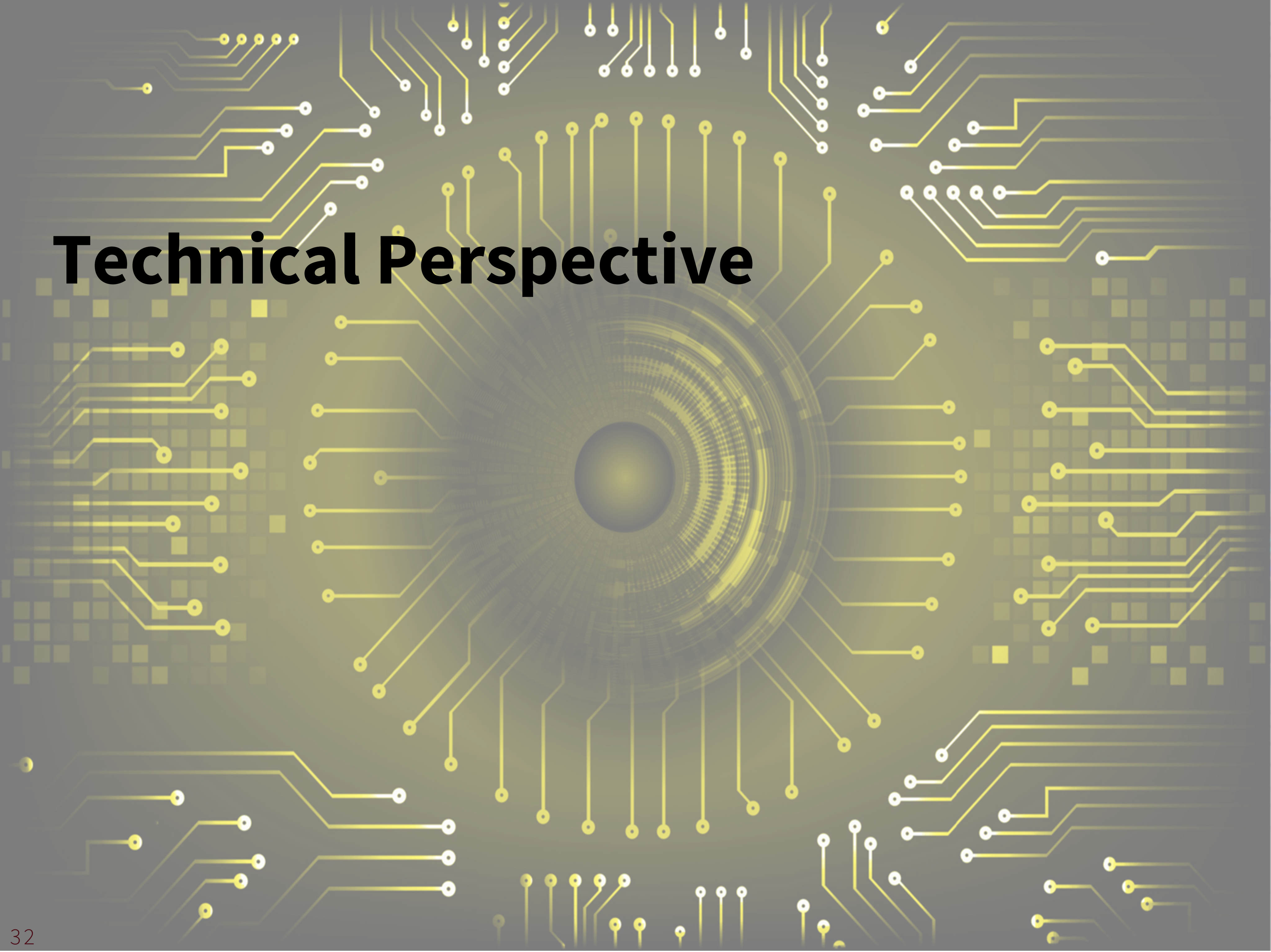
AmTrust FINANCIAL

THE HARTFORD

PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

Technical Perspective



TECHNICAL PERSPECTIVE

- Threat Landscape
- Security Technologies
- Security Practices
- Emerging Concerns

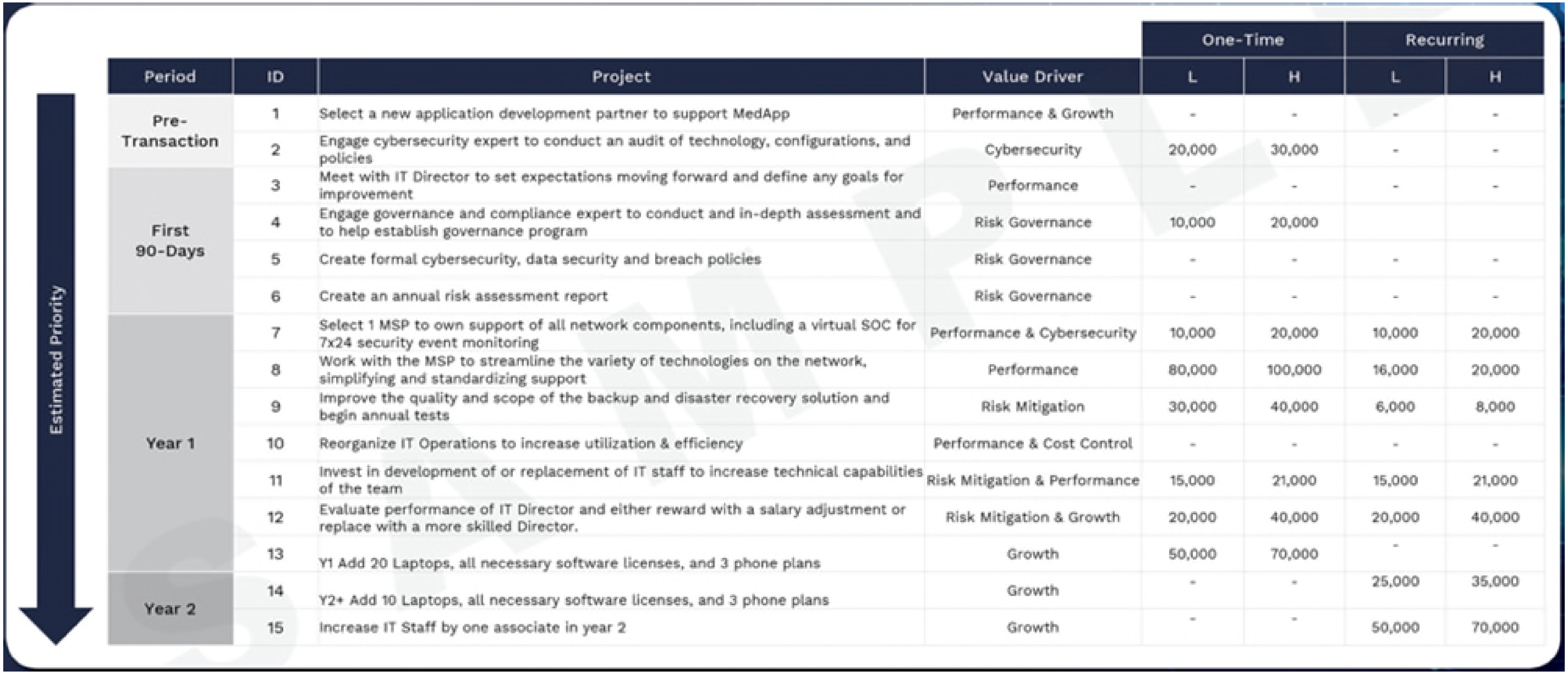
Security Posture Best Practices & Tools to Minimize Risk

- Security Awareness training
- Patch and software updates
- Endpoint protection
- Authentication & Access Control
- Backup and DR
- Vulnerability Management
- Incident response
- Regular Audits and Assessments

Assessing IT Due Diligence
Risk Maturity and Impact on Valuation

- Risk Evaluation
- Maturity Assessment
- Valuation Implications
- Strategic Importance

Based on risk assessment, create a remediation. Prioritize risk.



Estimated Priority

				One-Time		Recurring	
Period	**ID**	**Project**	**Value Driver**	**L**	**H**	**L**	**H**
Pre-Transaction	1	Select a new application development partner to support MedApp	Performance & Growth	-	-	-	-
	2	Engage cybersecurity expert to conduct an audit of technology, configurations, and policies	Cybersecurity	20,000	30,000	-	-
First 90-Days	3	Meet with IT Director to set expectations moving forward and define any goals for improvement	Performance	-	-	-	-
	4	Engage governance and compliance expert to conduct and in-depth assessment and to help establish governance program	Risk Governance	10,000	20,000		
	5	Create formal cybersecurity, data security and breach policies	Risk Governance	-	-	-	-
	6	Create an annual risk assessment report	Risk Governance	-	-	-	-
Year 1	7	Select 1 MSP to own support of all network components, including a virtual SOC for 7x24 security event monitoring	Performance & Cybersecurity	10,000	20,000	10,000	20,000
	8	Work with the MSP to streamline the variety of technologies on the network, simplifying and standardizing support	Performance	80,000	100,000	16,000	20,000
	9	Improve the quality and scope of the backup and disaster recovery solution and begin annual tests	Risk Mitigation	30,000	40,000	6,000	8,000
	10	Reorganize IT Operations to increase utilization & efficiency	Performance & Cost Control	-	-	-	-
	11	Invest in development of or replacement of IT staff to increase technical capabilities of the team	Risk Mitigation & Performance	15,000	21,000	15,000	21,000
	12	Evaluate performance of IT Director and either reward with a salary adjustment or replace with a more skilled Director.	Risk Mitigation & Growth	20,000	40,000	20,000	40,000
	13	Y1 Add 20 Laptops, all necessary software licenses, and 3 phone plans	Growth	50,000	70,000	-	-
Year 2	14	Y2+ Add 10 Laptops, all necessary software licenses, and 3 phone plans	Growth	-	-	25,000	35,000
	15	Increase IT Staff by one associate in year 2	Growth	-	-	50,000	70,000

TECHNICAL PERSPECTIVE

People

- Training and awareness
- Role Based Access
- Security-focused team
- Executive and Leadership adoption

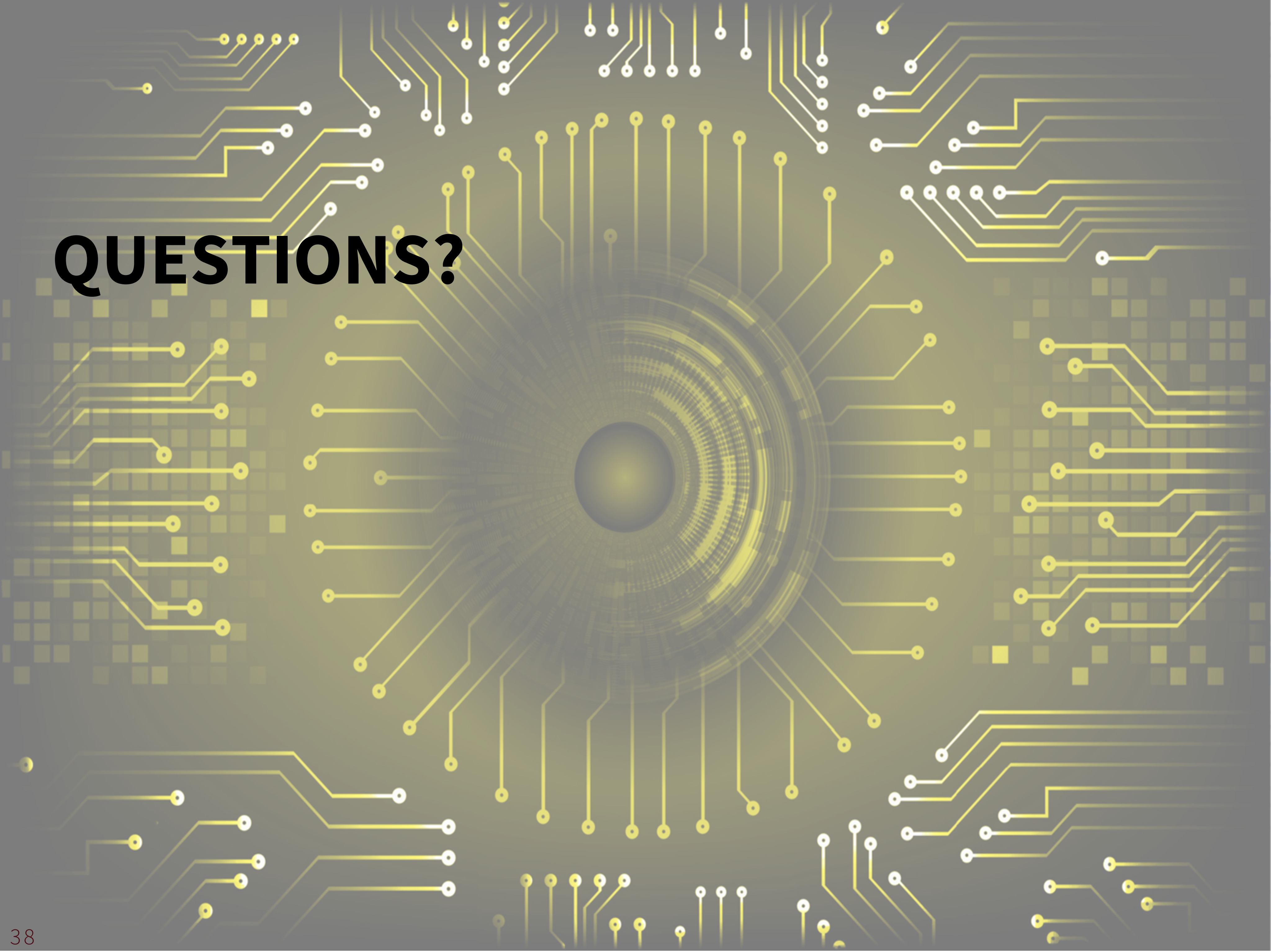
Process

- Incident response
- Regular Audits
- Patch Management
- Access Control
- Backup and DR
- Vendor management
- Regulatory

Technology

- Endpoint
- Encryption
- MFA
- IDPS
- SIEM
- Vulnerability
- Management
- AI

QUESTIONS?



This presentation is intended to provide general information. It is not intended as a form of, or as a substitute for, legal advice and analysis. Legal advice should always come from in-house or retained counsel. Moreover, if this presentation in any way contradicts advice of counsel, counsel's opinion should control over anything written herein. No attorney-client relationship is created or implied by this presentation. No reproduction or dissemination of this presentation is permitted without the prior written consent from Brach Eichler, LLC. @2022 Brach Eichler. All rights reserved.