MARYLAND
Health Care
Commission

Cyber Liability Insurance

What Practices Need to Know about Risk, Selecting Coverage, and Avoiding Common Pitfalls

FEBRUARY 18, 2022

About MHCC

WHO WE ARE

- Independent State regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment

WHAT WE DO

- Provide timely and accurate information on availability, cost, and quality of health care services to policy makers, purchasers, providers, and the public
- Advance health information technology (health IT) and innovative care delivery statewide

HOW WE HELP

- Educate providers and consumers on the value of and best practices for using health IT
- Includes raising awareness and sharing best practices about cybersecurity

Agenda

Welcome and Overview of the Cybersecurity Landscape

Justine Springer

Program Manager, Maryland Health Care Commission

Understanding and Managing Cyber Threats

Hear about the greatest cyber threats, potential damage of these threats, strategies to mitigate cyber risk, and steps practices can take to minimize disruption to practice operations and protect patient data.

David Greber

Principal, Offit Kurman, P.A.

Navigating the Purchase of Cybersecurity Insurance

Learn how to evaluate the different types of cyber liability coverage, select the right amount of coverage, and tips for completing questionnaires required by carriers.

Steve Rutkovitz

Chief Executive Officer, Choice Cybersecurity

Q & A

CME and Disclosures

- This activity has been planned and implemented in accordance with the Essential Areas and policies of the Accreditation Council for Continuing Medical Education (ACCME) through the joint providership of MedChi, The Maryland State Medical Society, and the Maryland Health Care Commission. MedChi is accredited by the ACCME to provide continuing medical education for physicians
- MedChi designates this virtual online activity for a maximum of 1 AMA PRA Category 1 Credits™
- Physicians should claim only the credit commensurate with the extent of their participation in the activity
- Presenters Justine Springer, Steve Rutkovitz, and David Greber have reported no relevant financial relationships with ineligible companies to disclose
- Planners for this activity have reported no relevant financial relationships with ineligible companies to disclose. The reviewers from MedChi's Committee On Scientific Activities have reported no relevant financial relationships with ineligible companies to disclose

Overview of the Cybersecurity Landscape

Cybersecurity in Health Care

- Health care cyber-attacks continue to increase with cyber criminals seeking to target unguarded or insufficiently guarded data
  - Ransomware (malicious software) and phishing attacks are most common
- Cyber-attacks that disrupt the ability to deliver care to patients and pose risks to patient safety are a key concern for health care practices
  - Cybercriminals anywhere in the world only need a computer and internet connection to disrupt operations and cause harm
- Privacy and security are interrelated but very distinct
  - Bolstering security of patient information improves patient privacy

Why Cybersecurity Matters

- Five years ago (2017), 8 in 10 physicians reported some form of a cyber-attack[1]
  - Reported breaches (>500 individuals) have nearly doubled since 2017[2]
- Cyber-attacks can result in identity theft, extortion attempts, the loss of important data like patient and financial records, regulatory fines and investigations (HIPAA), recovery costs, and reputational damage

1. American Medical Association. 8 in 10 doctors have experienced a cyberattack in practice, December 2017. Available at: www.ama-assn.org/practice-management/sustainability/8-10-doctors-have-experienced-cyberattack-practice
2. A total of 353 breaches reported in 2017 and 646 reported in 2020 for all covered entity (CE) types (heath plan, provider, and business associate).

Sources: mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Health_Care_Data_Breaches_Rpt.pdf
mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Health_Care_Data_Breaches_Rpt_012120.pdf

Do You Need Cyber Liability Insurance?

- Most likely -- insurance does not replace the need for implementing cybersecurity best practices; it complements good cybersecurity!
- Don’t assume your practice is too small to be targeted
  - A small practice can accumulate thousands of patient records over several years
- Cyber liability insurance can be personalized covering a broad range of risks and be based on security posture

Understanding and Managing Cyber Threats

David Greber

Principal, Offit Kurman, P.A.

Understanding and Managing Cyber Threats

Maryland Health Care Commission

Lunch and Learn Webinar

February 18, 2022

Dave Greber, CIPM, CIPP/US, CIPP/E

Offit | Kurman
Attorneys At Law

Dave Greber's Bio

Principal, Offit Kurman, P.A.

IAPP Certifications:

CIPM (Certified Information Privacy Manager)

CIPP/US (Certified Information Privacy Professional / US law)

CIPP/E (Certified Information Privacy Professional / European law)

Email: dgreber@offitkurman.com
Phone: 240.772.5137
Mailing: 50 Carroll Creek Way, Suite 340
Frederick , MD 21701
LinkedIn: David Greber

Offit | Kurman
Attorneys At Law

Definitions and Consequences

Cyber Threat (Data Breach) Defined:

- Unauthorized people have access to regulated personal information (PHI / PII)
- Includes Ransomware Attack: Information / computer systems locked and held for ransom

Cyber Threat Consequence:

- Costs of analyzing and "fixing" the problem
- Costs of notifying affected data subjects
- Potential regulatory fines / lawsuits
- Loss of business reputation / patients

Offit | Kurman
Attorneys At Law

Cyber Threat Quantified

Size of Threat ($) = Probability of Cyber Attack x Cost of Cyber Attack ($)

Offit | Kurman
Attorneys At Law

Probability of Cyber Attack

Healthcare industry is the main victim of data breaches*:

- 76.59% of all data breaches involved healthcare service providers (2015 – 2019)
- 255.18 million health records exposed (2010 – 2019)
- Hacking incidents dramatically increasing in healthcare

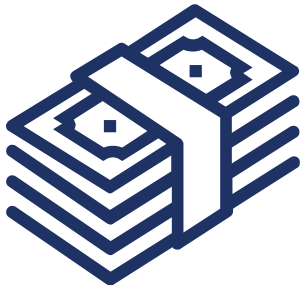
* Seh, Adil Hussain, et al., Healthcare Data Breaches: Insights and Implications (13 May 2020), www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

Offit | Kurman
Attorneys At Law

Cost of Cyber Attack

Healthcare: Highest Cost!*

$429 per breached record (2019)



* Seh, Adil Hussain, et al., Healthcare Data Breaches: Insights and Implications (13 May 2020), www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

Offit | Kurman
Attorneys At Law

Potential Damage of Cyber Attack

Doing the Math:

- Assume one doctor with a panel of 2,000 patients
- Assume cost per breached record = $500
- 2,000 patients x $500 = $1,000,000 damage
- If loss not survivable, risk mitigation crucial

Offit | Kurman
Attorneys At Law

Mitigation and Prevention Strategies

1. Cyber Insurance.

    - Use a knowledgeable insurance broker to evaluate policies
    - Understand the types of coverage available

2. Conduct a Comprehensive Risk Assessment.

    - Use a knowledgeable consultant
    - Required under HIPAA
    - Loads of information and tools available on HHS website (hhs.gov/hipaa/for-professionals/index.html)

3. Prioritize Measures that Address the Most Likely Risks.

Offit | Kurman
Attorneys At Law

Most Likely Risks (2015-2019)*

Type of Breach	%	Prevention Strategy
Hacking or Malicious Attacks --Email --Network Server	92.59%	Encryption Firewalls Passwords Software Updates Employee Training --Privacy Policy --Automated Training
Unintentional Disclosure	4.16%	Employee Training
Physical Damage such as theft or loss of paper documents	2.78%	Document Retention Policy

* Seh, Adil Hussain, et al., Healthcare Data Breaches: Insights and Implications (13 May 2020), www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

Offit | Kurman
Attorneys At Law

Avoid Disruption Post Breach and Protect Patient Data

- Excellent Data Back-up Routine
- Written Incident Response Plan
  --Note: First call is to cyber insurance company
- “Fire Drill”: Table-Top Exercise Simulating Breach

Offit | Kurman
Attorneys At Law

Navigating the Purchase of Cybersecurity Insurance

Steve Rutkovitz

CEO and Founder of Choice Cybersecurity

CHOICE CYBERSECURITY

Cyber Liability Insurance What Practices Need to Know about Risk, Selecting Coverage, and Avoiding Common Pitfalls.

STEVE RUTKOVITZ

CO-FOUNDER & CEO

ABOUT STEVE RUTKOVITZ

For over 20 years, Steve owned and operated a very successful MSP business specializing in medical systems. With a clear understanding of the market needs, he developed an innovative Security and Compliance business process.

- Security and Compliance
- Risk Assessments
- Education
- HIPAA Compliance

CHOICE CYBERSECURITY

STATE OF CYBER SECURITY

61%

SMBs

61% of all security breaches target SMBs

50%

2021

50% increase in cyber attacks

76%

PHISHING

76% of businesses reported phishing attacks

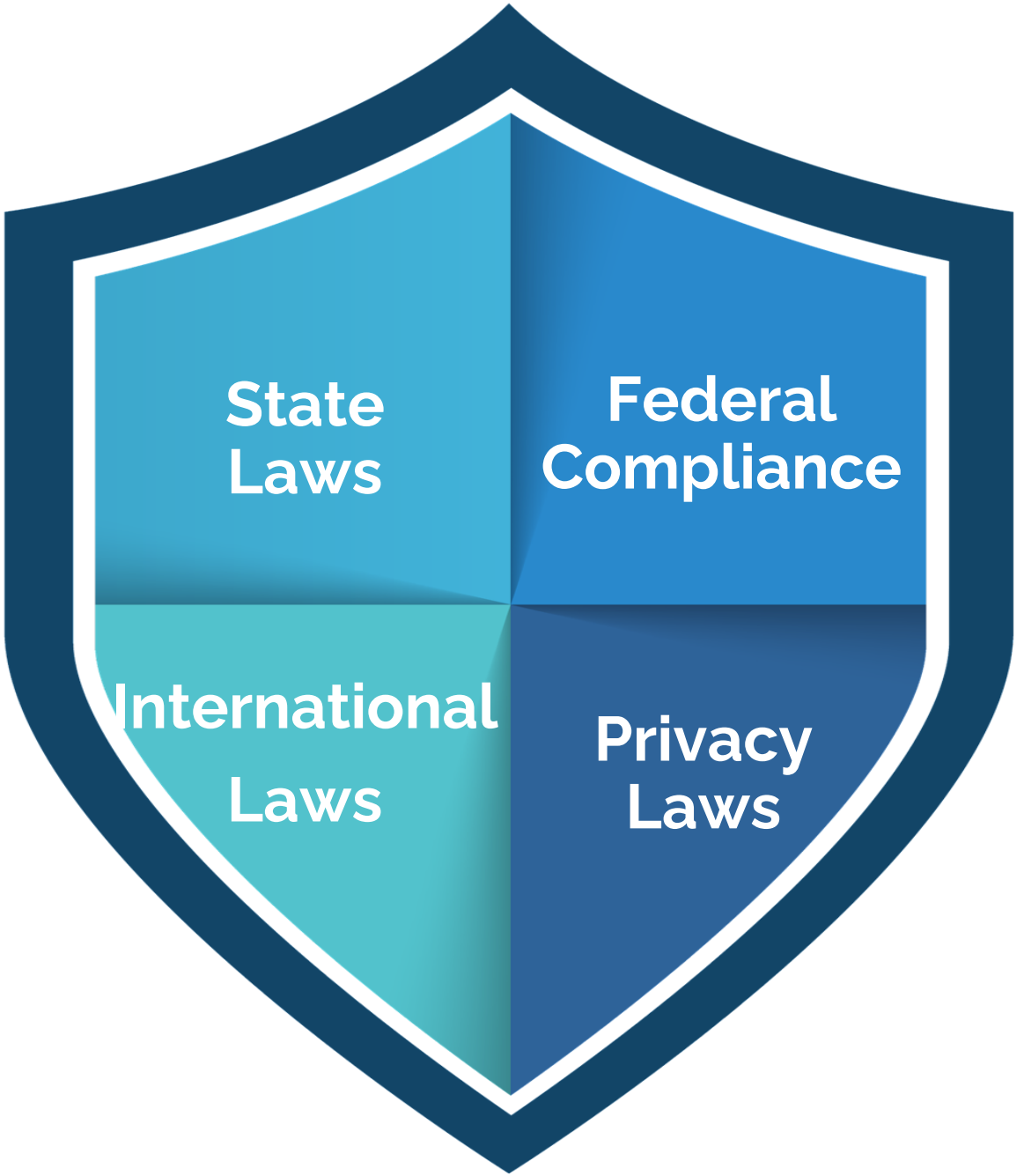
600%

IOT

Attacks increased by 600%

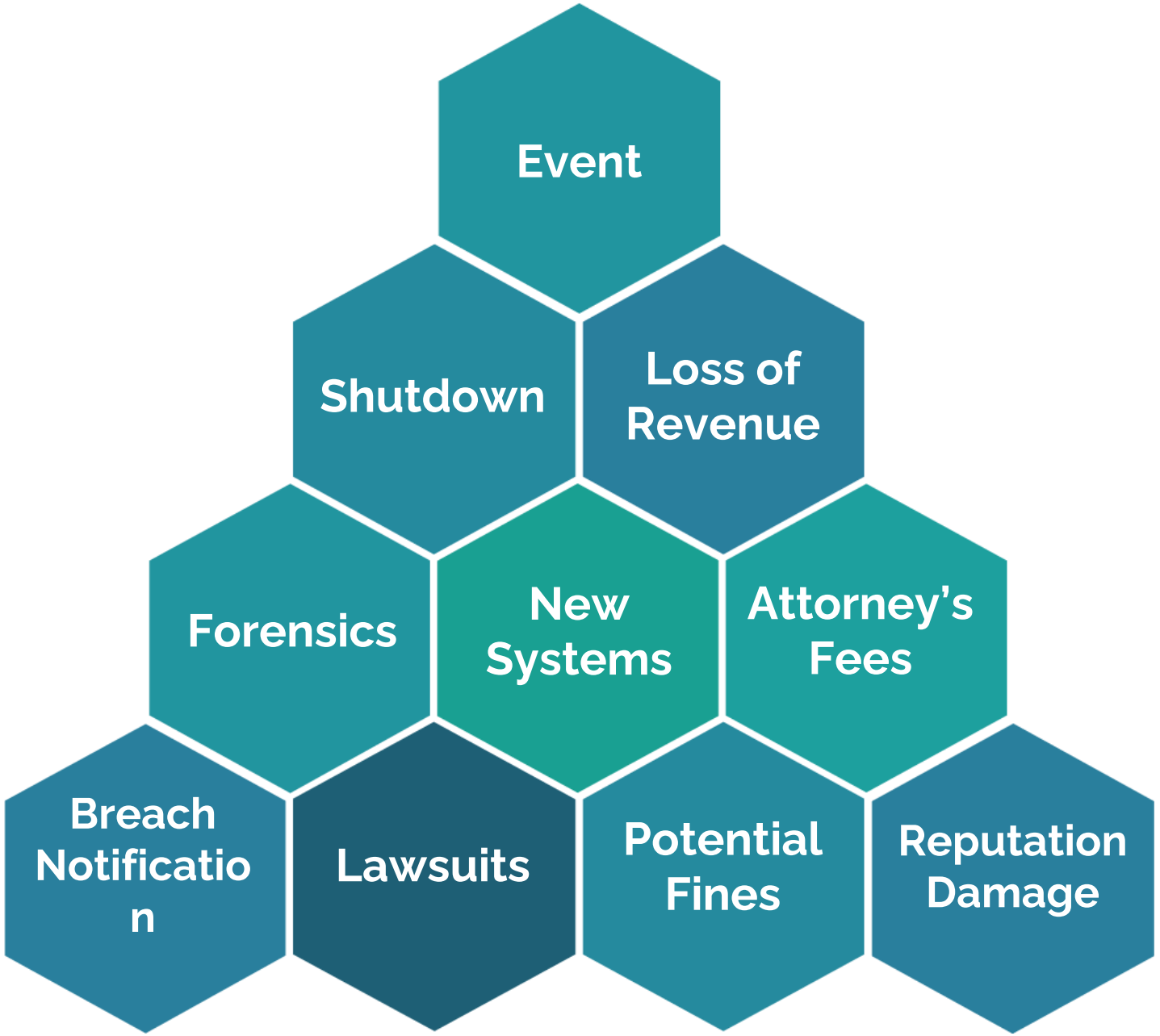
COMPLIANCE & BEST PRACTICES

- State
- HIPAA
- PCI
- Privacy

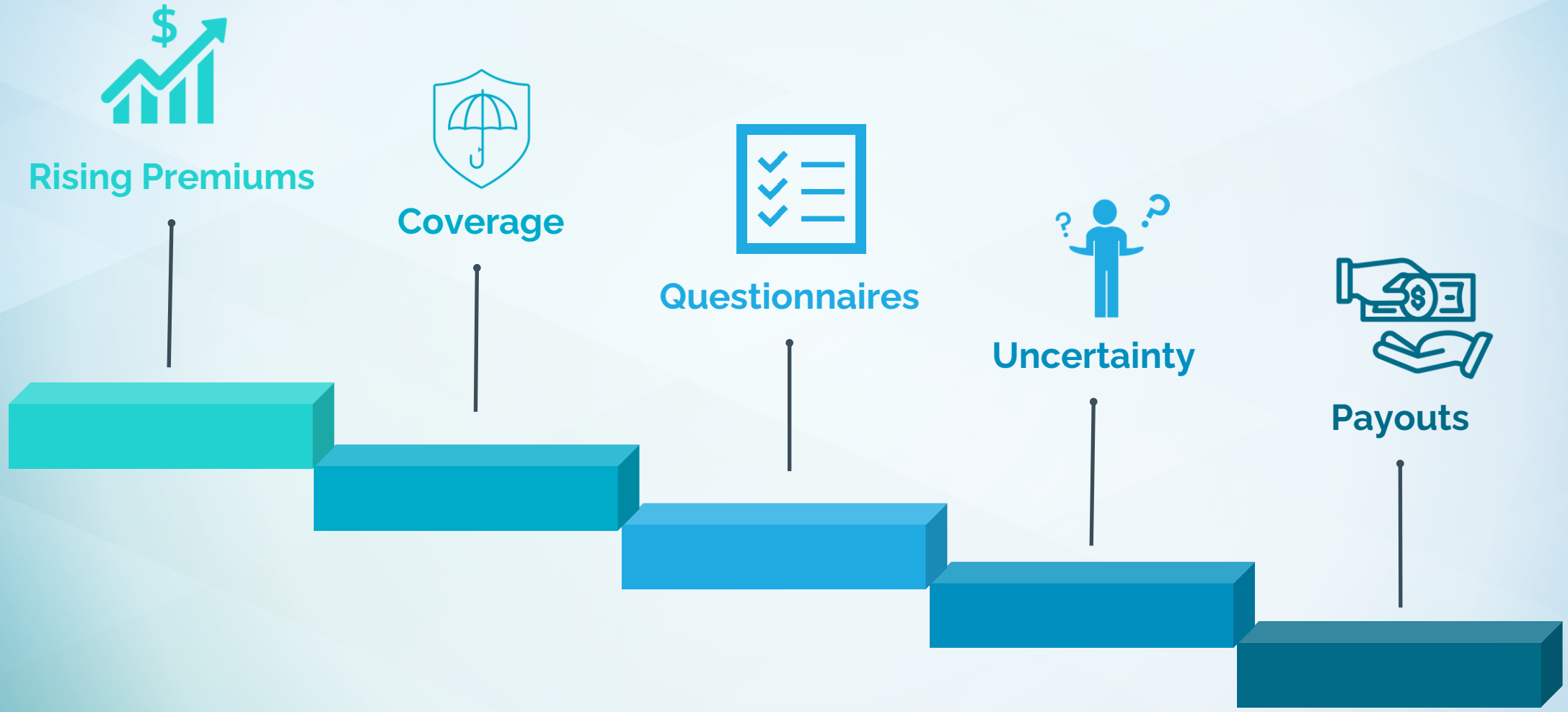


Breach Unfolding

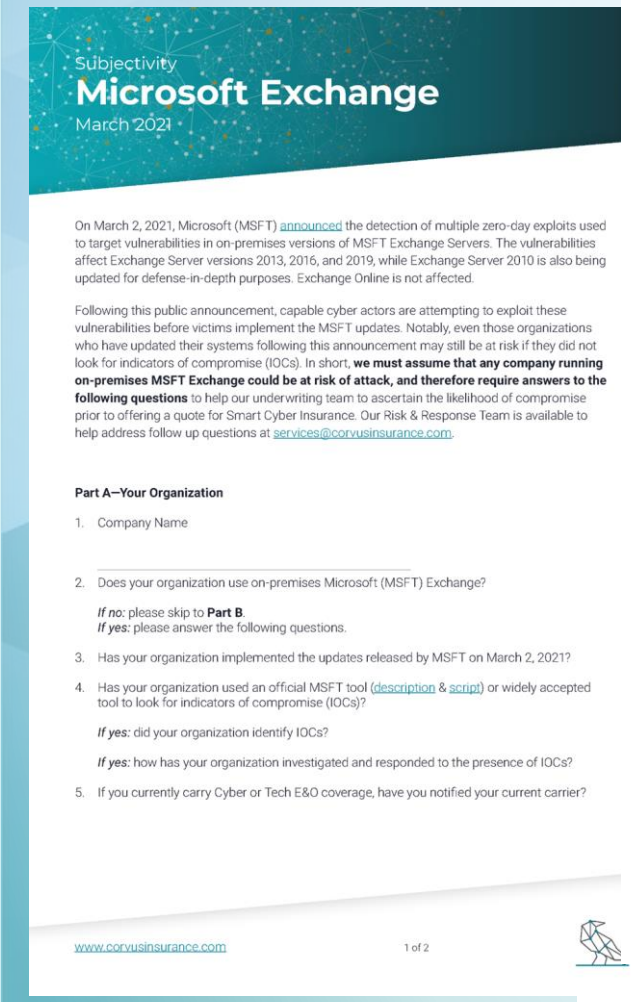
- Average Breach $1.8 million+



CYBER INSURANCE TODAY



Cyber Insurance Forms



Subjectivity

Microsoft Exchange

March 2021

On March 2, 2021, Microsoft (MSFT) announced the detection of multiple zero-day exploits used to target vulnerabilities in on-premises versions of MSFT Exchange Servers. The vulnerabilities affect Exchange Server versions 2013, 2016, and 2019, while Exchange Server 2010 is also being updated for defense-in-depth purposes. Exchange Online is not affected.

Following this public announcement, capable cyber actors are attempting to exploit these vulnerabilities before victims implement the MSFT updates. Notably, even those organizations who have updated their systems following this announcement may still be at risk if they did not look for indicators of compromise (IOCs). In short, **we must assume that any company running on-premises MSFT Exchange could be at risk of attack, and therefore require answers to the following questions** to help our underwriting team to ascertain the likelihood of compromise prior to offering a quote for Smart Cyber Insurance. Our Risk & Response Team is available to help address follow up questions at services@corvusinsurance.com.

Part A—Your Organization

1. Company Name

2. Does your organization use on-premises Microsoft (MSFT) Exchange?

   If no: please skip to **Part B**.
   If yes: please answer the following questions.

3. Has your organization implemented the updates released by MSFT on March 2, 2021?

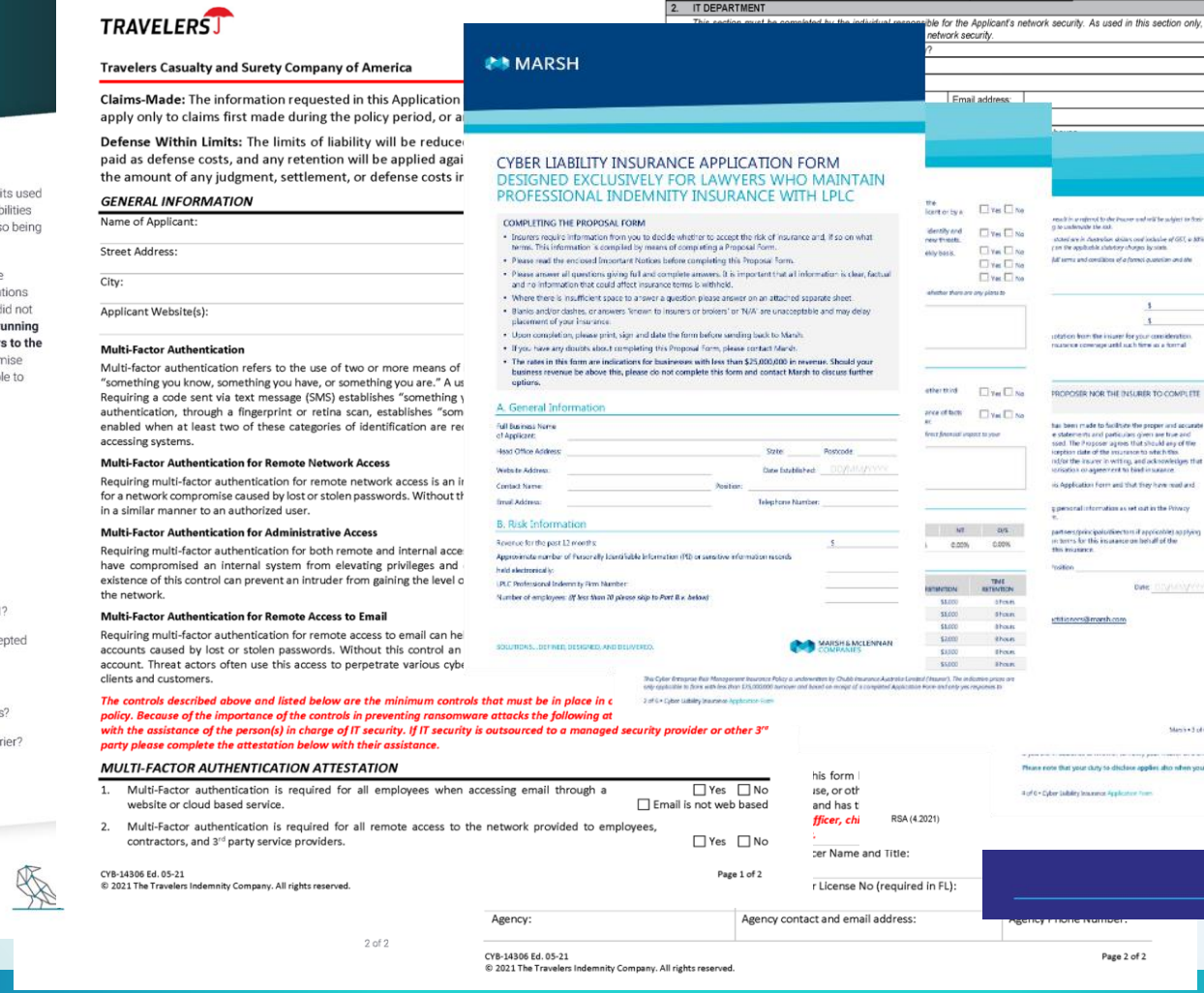
4. Has your organization used an official MSFT tool (description & script) or widely accepted tool to look for indicators of compromise (IOCs)?

   If yes: did your organization identify IOCs?

   If yes: how has your organization investigated and responded to the presence of IOCs?

5. If you currently carry Cyber or Tech E&O coverage, have you notified your current carrier?

www.corvusinsurance.com 1 of 2



TRAVELERS

Travelers Casualty and Surety Company of America

Claims-Made: The information requested in this Application apply only to claims first made during the policy period, or a

Defense Within Limits: The limits of liability will be reduce paid as defense costs, and any retention will be applied agai the amount of any judgment, settlement, or defense costs ir

GENERAL INFORMATION

Name of Applicant:

Street Address:

City:

Applicant Website(s):

Multi-Factor Authentication

Multi-factor authentication refers to the use of two or more means of "something you know, something you have, or something you are." A us Requiring a code sent via text message (SMS) establishes "something authentication, through a fingerprint or retina scan, establishes "som enabled when at least two of these categories of identification are re accessing systems.

Multi-Factor Authentication for Remote Network Access

Requiring multi-factor authentication for remote network access is an i for a network compromise caused by lost or stolen passwords. Without th in a similar manner to an authorized user.

Multi-Factor Authentication for Administrative Access

Requiring multi-factor authentication for both remote and internal acce have compromised an internal system from elevating privileges and existence of this control can prevent an intruder from gaining the level o the network.

Multi-Factor Authentication for Remote Access to Email

Requiring multi-factor authentication for remote access to email can he accounts caused by lost or stolen passwords. Without this control an account. Threat actors often use this access to perpetrate various cybe clients and customers.

The controls described above and listed below are the minimum controls that must be in place in c policy. Because of the importance of the controls in preventing ransomware attacks the following at with the assistance of the person(s) in charge of IT security. If IT security is outsourced to a managed security provider or other 3rd party please complete the attestation below with their assistance.

MULTI-FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing email through a website or cloud based service. ☐ Yes ☐ No ☐ Email is not web based

2. Multi-Factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☐ Yes ☐ No

CYB-14306 Ed. 05-21
© 2021 The Travelers Indemnity Company. All rights reserved.

Page 1 of 2

2 of 2

MARSH

CYBER LIABILITY INSURANCE APPLICATION FORM
DESIGNED EXCLUSIVELY FOR LAWYERS WHO MAINTAIN PROFESSIONAL INDEMNITY INSURANCE WITH LPLC

COMPLETING THE PROPOSAL FORM

- Insurers require information from you to decide whether to accept the risk of insurance and, if so on what terms. This information is compiled by means of completing a Proposal Form.
- Please read the enclosed Important Notices before completing this Proposal Form.
- Please answer all questions giving full and complete answers. It is important that all information is clear, factual and no information that could affect insurance terms is withheld.
- Where there is insufficient space to answer a question please answer on an attached separate sheet.
- Blanks and/or dashes, or answers 'known to insurers or brokers' or 'N/A' are unacceptable and may delay placement of your insurance.
- Upon completion, please print, sign and date the form before sending back to Marsh.
- If you have any doubts about completing this Proposal Form, please contact Marsh.
- **The rates in this form are indicators for businesses with less than $25,000,000 in revenue. Should your business revenue be above this, please do not complete this form and contact Marsh to discuss further options.**

A. General Information

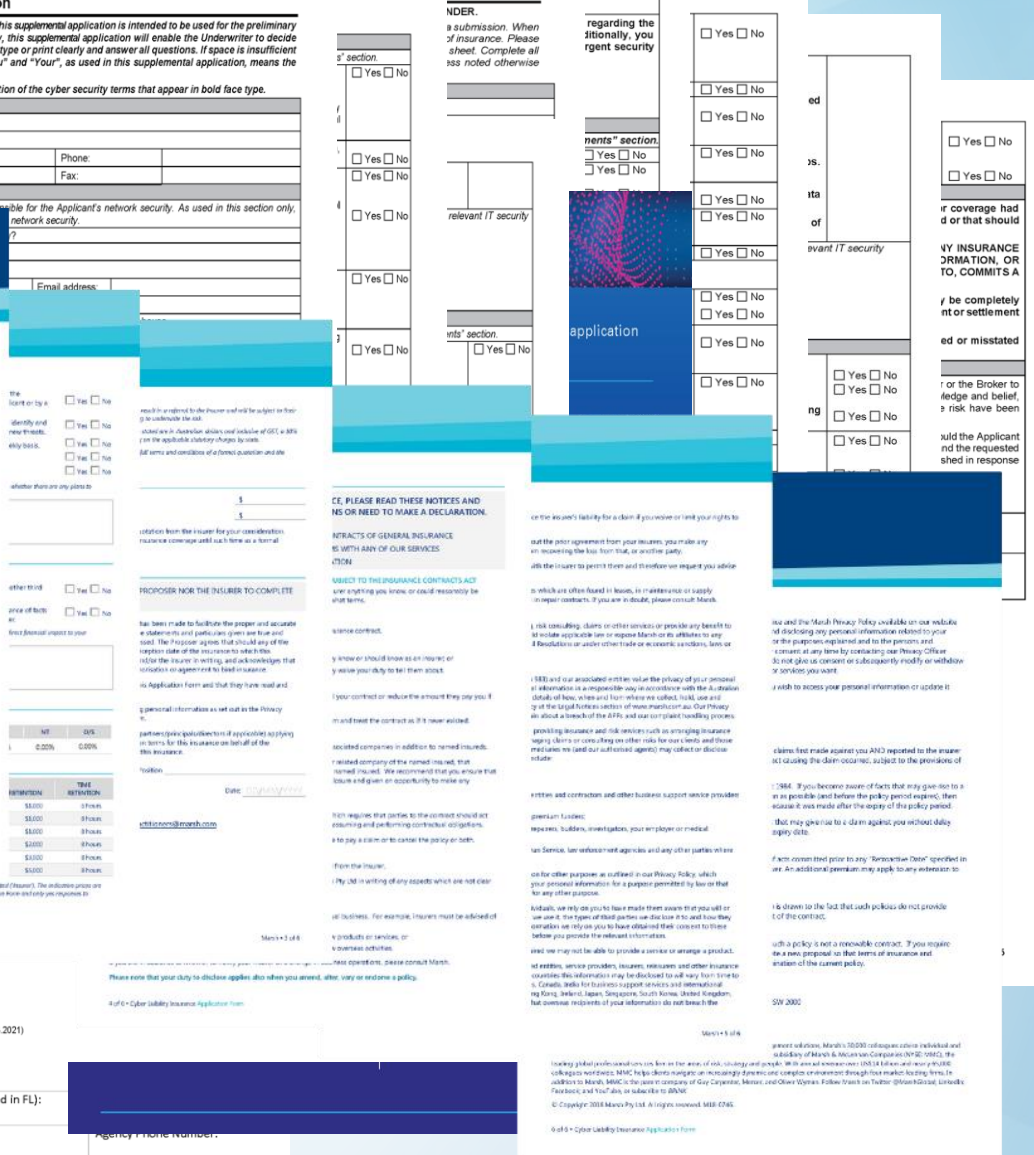
Full Business Name of Applicant:
Head Office Address: State: Postcode:
Web site Address: Date Established:
Contact Name: Position:
Email Address: Telephone Number:

B. Risk Information

Revenue for the past 12 months: $
Approximate number of Personally Identifiable Information (PII) or sensitive information records held electronically:
LPLC Professional Indemnity Firm Number:
Number of employees: *(If less than 20 please skip to Part B v. below)*

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES



TOKIO MARINE HCC

Cyber & Professional Lines Group
16501 Ventura Blvd. Suite 200, Encino, CA 91436
main (818) 382-2030
tmhcc.com/pro

Ransomware Supplemental Application

THIS SUPPLEMENTAL APPLICATION IS NOT A BINDER. *This supplemental application is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this supplemental application will enable the Underwriter to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. "You" and "Your", as used in this supplemental application, means the Applicant unless noted otherwise below.*

Please refer to the attached Cyber Glossary for an explanation of the cyber security terms that appear in bold face type.

1. GENERAL INFORMATION			
Name of Applicant:			
Street Address:			
City, State, Zip:		Phone:	
Website:		Fax:	

2. IT DEPARTMENT
This section must be completed by the individual responsible for the Applicant's network security. As used in this section only, "you" and "your" means the Applicant's network security.
Name:
Title:
Phone: Email address:

Agency: Agency contact and email address: Agency Phone Number:

CYB-14306 Ed. 05-21
© 2021 The Travelers Indemnity Company. All rights reserved.

Page 2 of 2

CCS CHOICE CYBERSECURITY

CYBER RISK ALIGNMENT

Our Assessment Process

ASSESS

ADDRESS

MAINTAIN

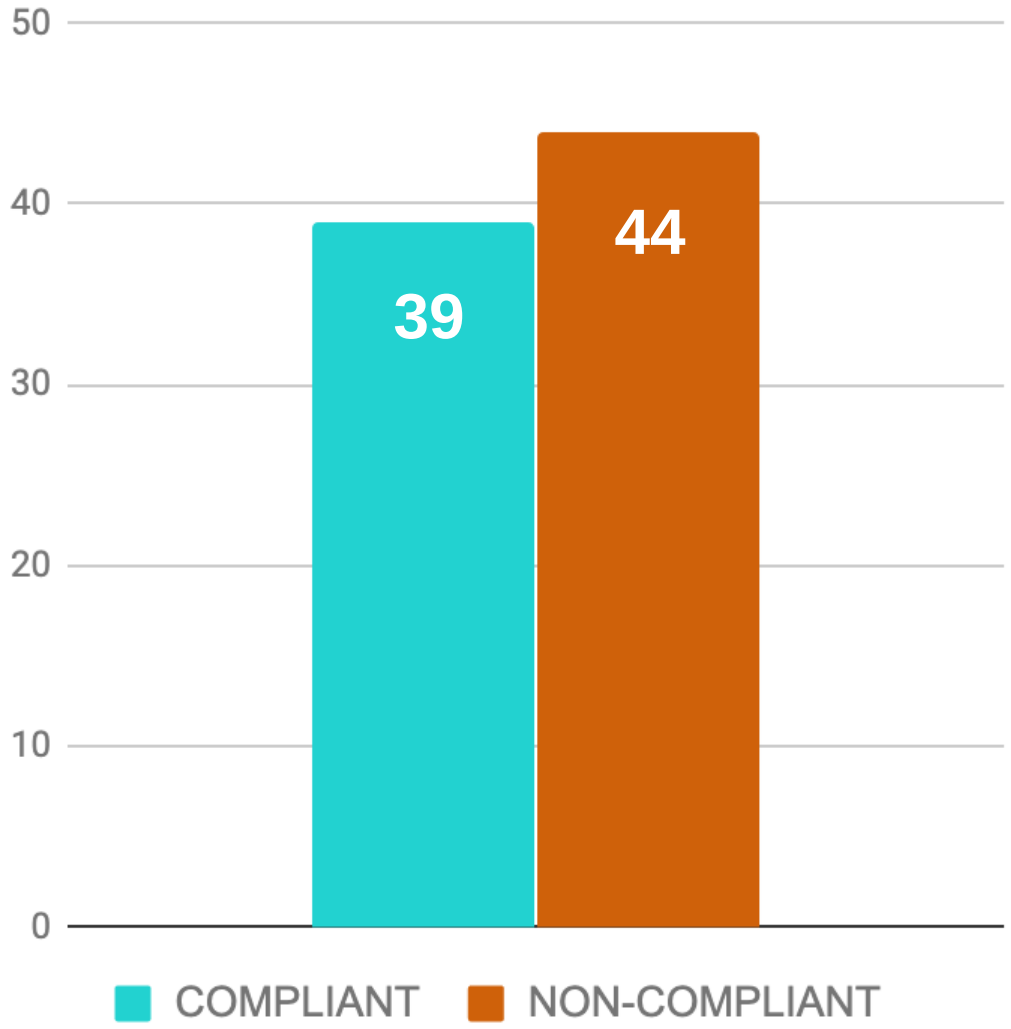
Risk Assessment Components

ePHI Scan Results and Data Auditing

TOTAL LIABILITY: $10,043,391

35,000	9,936	14,451	2,746
Medical Records	Credit Cards	Social Security Numbers	Dates of Birth

HIPAA REPORT ON COMPLIANCE

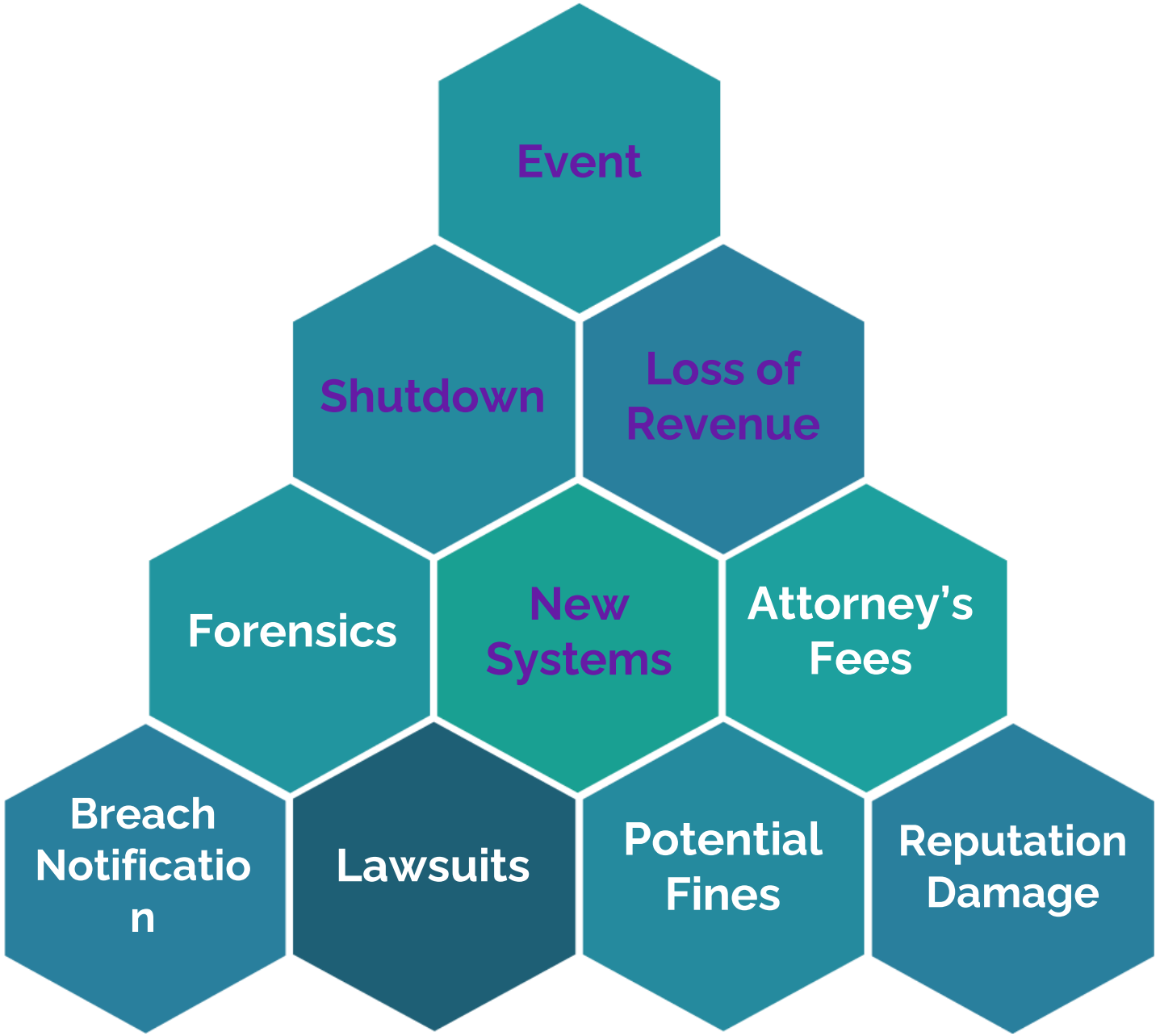


CONTROLS STATUS PER STANDARDS & REGULATIONS

SAFE HARBOR

Breach Unfolding with Safe Harbor

- Average Breach $1.8 million+
- Average Safe Harbor Breach less than $100,000



HOW TO BUY INSURANCE

1. Amount of Coverage
2. Coverage Terms
3. Premium
4. Deductible
5. Exclusions

Summary

- If you can do these three things than you are set

MARYLAND TAX PROGRAM

- <50 Employees
- For profit company
- 2022 Calendar year
- 50% Dollar for dollar tax credit

CHOICE CYBERSECURITY

info@choicecybersecurity.com

(410) 205-4980

www.choicecybersecurity.com

10065 Red Run Blvd
Suite 120
Owings Mills, MD 21117

Q&A

Resources

- Maryland Health Care Commission Cybersecurity Webpage
  mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/hit_cybersecurity.aspx
- Health Care Data Breaches, Perspectives on Breach Trends in Maryland and Comparative States
  mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Health_Care_Data_Breaches_Rpt.pdf
- Summary of the HIPAA Security Rule
  www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- HIPAA Safe Harbor Bill: Understanding What It Means for Your Practice
  www.hipaaexams.com/blog/hipaa-safe-harbor-bill-understanding-what-it-means-for-your-practice/
- 10 Practices to Protect Your Organization from Cyber Threats

  405d.hhs.gov/Documents/405d-infographic-10practices.pdf

Thank you!

Justine Springer

Program Manager

justine.springer@maryland.gov