# *Mitigating Cyber Risk Webcast*

## *In partnership with CrossFirst Bank*

Maryam Rad | Director of Business Operations | Cyber and Technology | Lockton

Tyler Klein | Practice Leader | Cyber and Technology | Lockton

Justin Corrado | Senior Vice President | Cyber and Technology | Lockton

LOCKTON

# *Exposures for public companies*

More securities litigation

Greater regulatory burdens

Spotlight on incidents

Loss of customers

Reputational risk

Drop in stock prices

More consumer class-action litigation

Claims of misrepresentations/deceptive business practices

# *Fundamentals of cyber risk management*

## 01

### KNOW YOUR OPERATIONS

- What is critical?
- Where is crucial data stored?
- How will you respond in the event of an incident?
- How will an incident impact your employees, customers, and brand?
- How do your vendor relationships fit into the equation?

## 02

### BUILD A SECURITY CULTURE

- What are the organizational initiatives round building a security culture?
- Do those initiatives take into account the various teams and workstreams within your organization?
- What education and training practices does the organization employ?

## 03

### CROSS FUNCTIONAL PLAN

- Does the organization have a plan in the event of an incident?
- Does that plan contemplate business continuity?
- Have the appropriate stakeholder been accounted for in the planning?
- Has the organization tested the plan?

# *Increased activity*

**International, federal, state and local regulators continue to expand privacy protections around the globe. Significant regulatory activity includes:**

- European Union's General Data Protection Regulation
- China's Personal Information Protection Law and Data Security Law
- U.S. Treasury's Office of Foreign Assets control's updated advisory on ransomware payments
- State legislation, including:
  - California Consumer Privacy Act and California Privacy Rights Act
  - Virginia Consumer Data Protection Act
  - Colorado Privacy Act
  - Utah Consumer Privacy Act

**Some laws have been around for some time but have recently seen an increase in litigation and/or enforcement activity. Examples include:**

- Health Information Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Illinois Biometric Information Privacy Act (BIPA)
- Children's Online Privacy Protection Act (COPPA)
- Fair and Accurate Credit Transactions Act
- Regulation S-P
- Video Privacy Protection Act (VPPA)
- Federal and state wiretap laws

ENFORCEMENT agencies are entrusted to administer, investigate and impose consequences on organizations failing to comply with various privacy protections. Examples of enforcement agencies include:

- Data protection authorities
- U.S. Department of Health and Human Services, Office of Civil Rights
- Securities and Exchange Commission
- Federal Trade Commission
- State attorneys general

Liability for failure to comply with privacy protections can subject an organization to costly and lengthy litigation by third parties and/or proceedings initiated by the regulatory body claiming violations of various laws.

# *Cyber hygiene practices*

Enable multifactor authentication

Establish principle of least privilege

Utilize scanning and filtering solutions

Use antivirus software

Ensure firewall protections are in place

Implement endpoint detection and response (EDR) tools

Implement security monitoring solutions, such as security incident event management system and security operations center

Keep current backups off site, encrypted and regularly tested

Update hardware and software regularly, including implementing critical patches within two days

Segment the network

Create and test incident response and business continuity plans

Audit third-party vendors' cybersecurity practices

# *Education practices*

## *Employee & leadership training*

Educate employees not to click on links and open attachments

Conduct periodic testing of workforces' susceptibility to phishing attempts

Create an information governance plan and build a culture that supports the plan


Establish and promote good cyber hygiene

# *Cyber policies*

## FIRST-PARTY COVERAGES

Compensate insureds for their own losses resulting from covered cyber events. Claims may arise from breaches, suspected breaches, suspicious activity on networks and cyberattacks.

EXAMPLES INCLUDE:

- A stolen laptop with confidential information.
- A hacked computer system.
- Business email compromise caused by phishing.
- A ransomware attack.
- A denial-of-service attack.

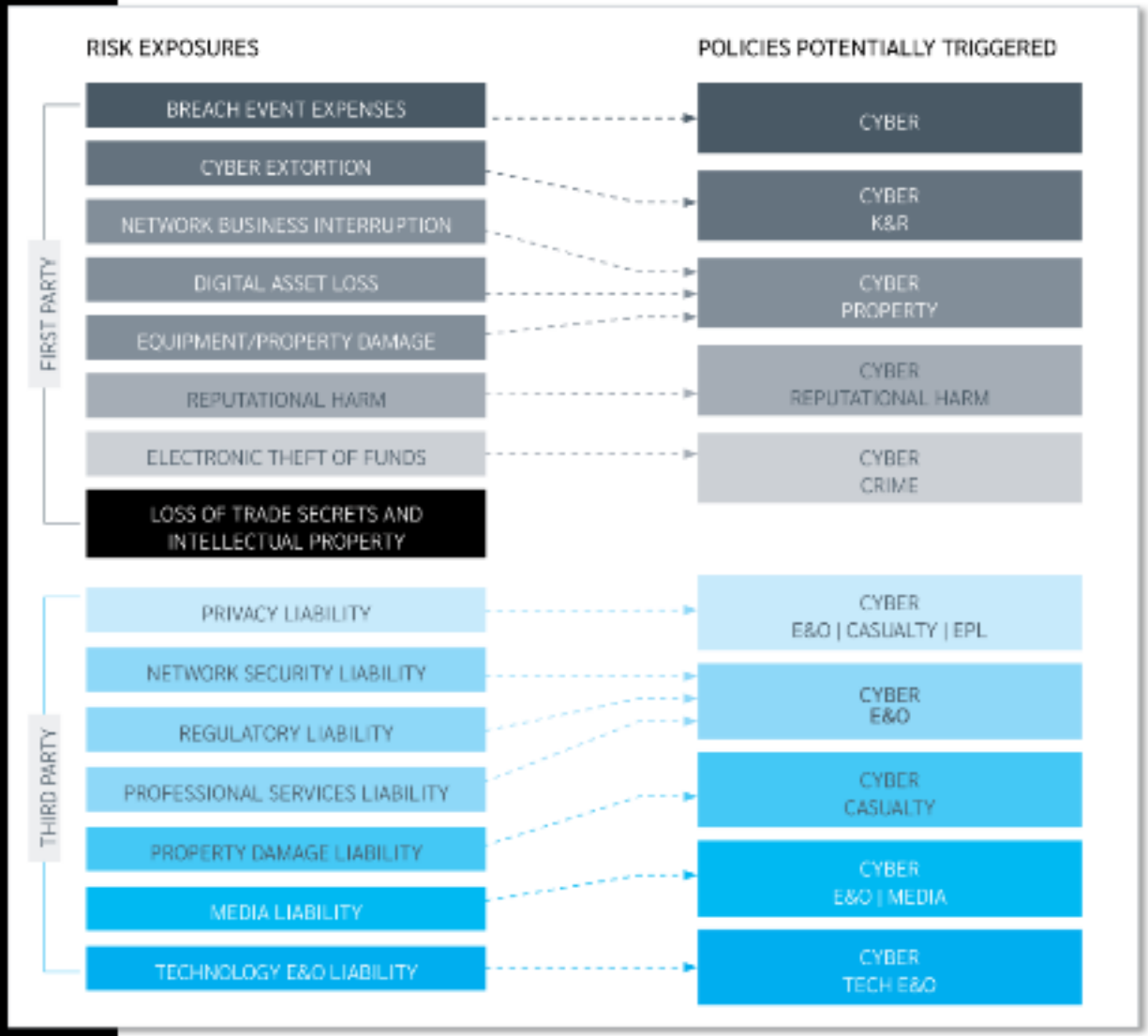
## THIRD-PARTY COVERAGES

Pay others for insureds' liability to them for losses arising from covered cyber events and/or wrongful act. Claims can include written demands, tolling agreements, arbitration demand, regulatory inquiries and complaints.

EXAMPLES INCLUDE:

- A demand for arbitration related to the disclosure of confidential information.
- A class-action complaint for violations of the laws that protect consumers' personally identifiable information.
- A regulatory inquiry regarding the organization's handling of confidential data.

# *Insurance & risk transfer*



# *Risk management – asking the right questions*

## QUANTITATIVE

| GEOGRAPHY & INDUSTRY | VALUE | DATA & INFORMATION | BUDGET |
|---|---|---|---|
| Does the organization's business and area(s) of operation fall into a heavily regulated or litigious jurisdiction? | Does the organization have digital assets, records, information and/or financial assets making it more susceptible to a cyberattack? | What are the organization's policies, procedures and protocols around data collection, retention, storage and destruction? | What has the organization committed in budget to cybersecurity and risk transfer mechanism? |

## QUALITATIVE

| INFORMATION TECHNOLOGY & SECURITY | PRIVACY | RISK TOLERANCE | MANAGEMENT | RESOURCES | CONTRACTUAL OBLIGATIONS |
|---|---|---|---|---|---|
| What is the organization's culture around information technology and security? | What are the organization's values around the protection of private and confidential information? | What is the organization's risk tolerance and philosophy around enterprise risk management? | What are management's principles around privacy, technology and information security? | What are the organization's values about committing funds to cybersecurity improvements and risk transfer mechanisms? | Does the organization maintain a consistent protocol to review and negotiate contracts that favor the organization? |

# *Thank you for joining us*


**Maryam Rad**
Director of Business Operations
Cyber and Technology
Lockton
+1.415.235.0934
mrad@lockton.com

**Tyler Klein**
Practice Leader
Cyber and Technology
Lockton
+1.816.960.9667
tklein@lockton.com

**Justin Corrado**
Senior Vice President
Cyber and Technology
Lockton
+1.484.880.5621
jcorrado@lockton.com


For more insights from Lockton

**Visit our website at lockton.com**

**Follow Lockton on LinkedIn**

*Independence changes everything.*

LOCKTON

UNCOMMONLY INDEPENDENT