

McDermott
Will & Emery

ACC Association of
Corporate Counsel
CHICAGO



DEMYSTIFYING CYBERSECURITY: PRACTICAL CONSIDERATIONS FOR BUSINESSES

December 8, 2021

aon.com
mwe.com



WELCOME AND SOME HOUSEKEEPING ITEMS

- Your environment should be free from distractions
- Be sure to mute your microphone if you are not speaking
- Ask questions! Our panelists are happy to engage with you
- If you didn't provide your IL ARDC number email ChicagoSupport@accglobal.com
- Watch for the survey/evaluation request sent to your email after the program

A REMINDER ABOUT THE BENEFITS OF ACC MEMBERSHIP...

- Free CLE, Roundtables, Women's & Professional Development Programs
- Socials, Pop Ups, Special Networking Groups, Annual Celebration Event
- Community Outreach, Diversity Initiatives & Pro Bono Offerings
- Leadership and Speaking Opportunities, Chicago Lawyer Subscription
- Access to ACC Global Resources, including:
 - ACC Docket Magazine & Newsstand (searchable legal news feed)
 - ACC Survey Portal, Resource Library, Contracts Portal & Legal Ops Section
 - E-Groups and Committees on Substantive Practice Areas

PRESENTERS



DAVID SAUNDERS

Partner

McDermott Will & Emery



DEEPALI DODDI

Associate

McDermott Will & Emery



KRISTA CATTANACH

Senior Privacy Counsel

Aon



AGENDA

- Cybersecurity Basics
- Cybersecurity Legal Landscape
- Building an Effective Cybersecurity Program
- Cybersecurity as a Competitive Differentiator
- Best Practices for Incident Response

CYBERSECURITY BASICS



WHAT IS PRIVACY? WHAT IS CYBERSECURITY?

Privacy

- Keep the government out of my private life and “the right to be let alone” Don’t engage in deceptive or unfair practices (consumer protection and consumer expectations)
- Protect my personal data and allow me to retain control of that data (data protection)









Cybersecurity

- Protect the confidentiality, integrity, and availability of the company’s information, systems, and networks



FULL SPECTRUM OF THREATS

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hackers use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

CYBERSECURITY LEGAL LANDSCAPE



CYBERSECURITY: WHAT IS LEGALLY REQUIRED?

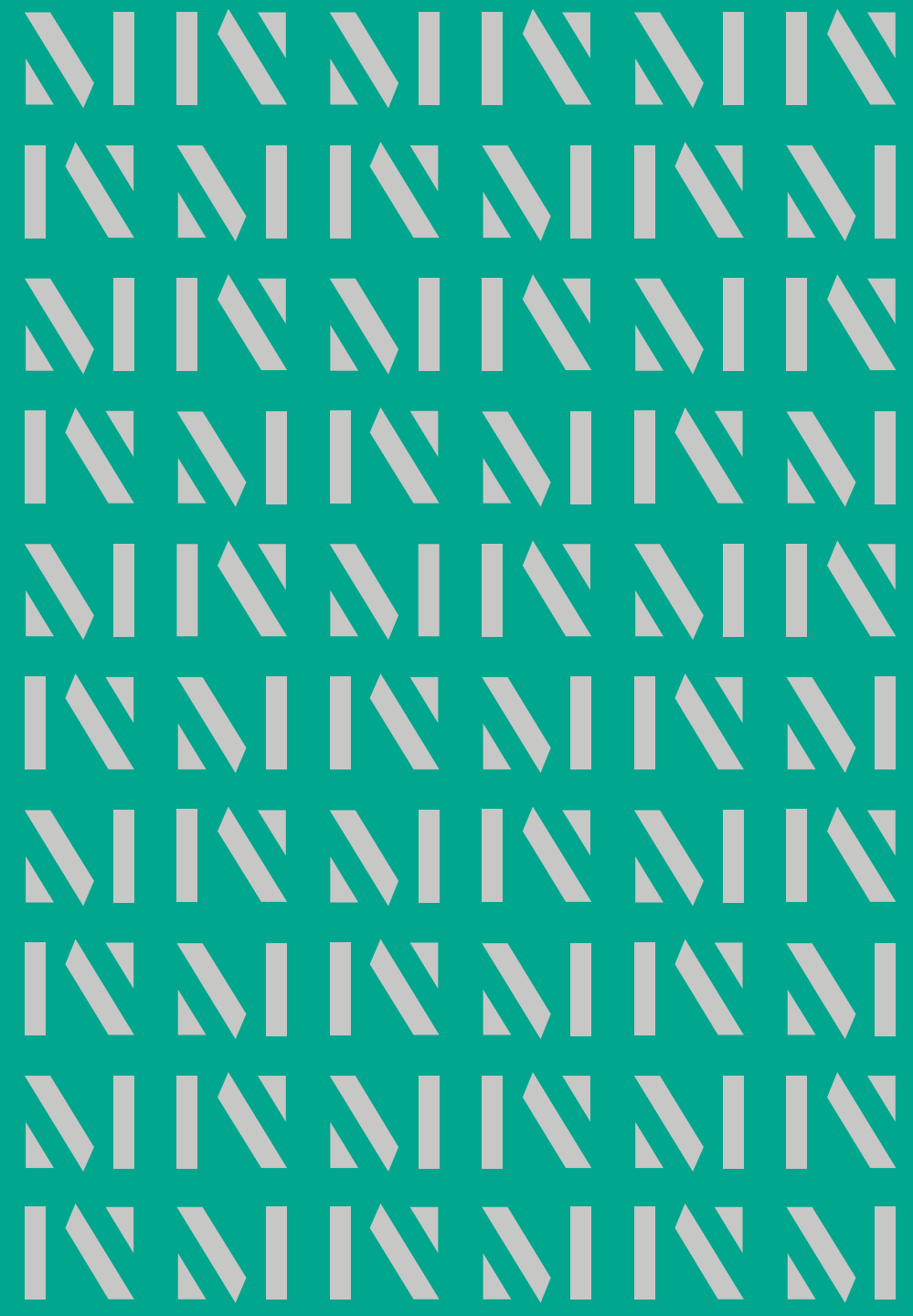
- Legal (not exhaustive)
 - Personal Information/Data
 - State laws requiring reasonable security safeguards and/or written information security programs (e.g., California Consumer Privacy Act, New York SHIELD Act, Massachusetts data security law)
 - Breach notification laws
 - Biometrics laws
 - Children (COPPA)
 - May 12, 2021, Executive Order on Improving the Nation's Cybersecurity
 - SEC (disclosure of material risks and incidents)
 - Common law (e.g., Torts)
 - FTC Act (prohibition against unfair or deceptive trade practices)
 - Industry specific laws (e.g., HIPAA, GLBA)
 - ERISA (cybersecurity as a fiduciary duty)
 - Computer Fraud and Abuse Act
 - Sarbanes-Oxley (financial controls)
 - Board obligations
 - International laws (e.g., GDPR, China Cybersecurity Law)

CYBERSECURITY LANDSCAPE

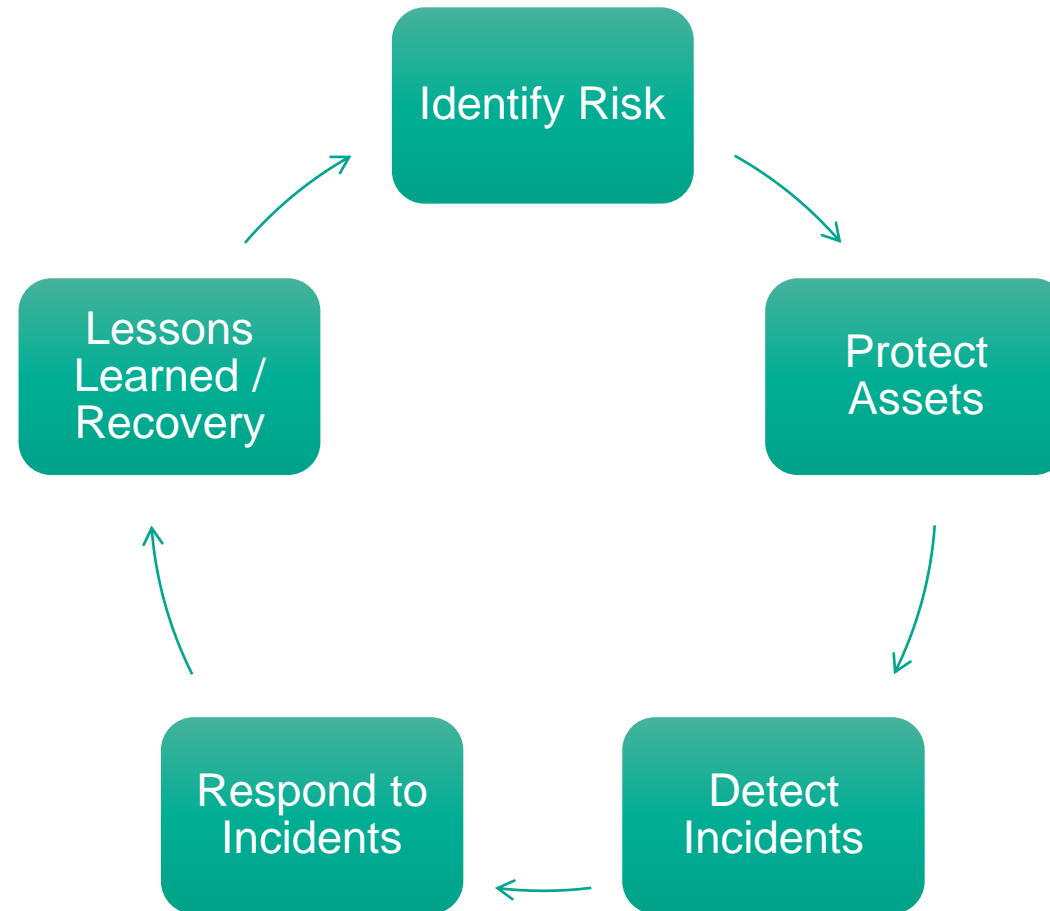
KEY CONCEPTS AND TRENDS

- “Reasonable Security”
 - Vague standard under continuous and evolving interpretation by regulators and courts
 - As enforced, regulators expect a risk-based approach to cybersecurity
- Current Trend: **Granularity**
 - Massachusetts: Must have a “written information security program”
 - California Privacy Rights Act: Security assessments
- **Privacy Laws**
 - e.g., requirements for role-based access to data

BUILDING AN EFFECTIVE CYBERSECURITY PROGRAM



CYCLE OF CYBERSECURITY



CYBERSECURITY PROGRAM BEST PRACTICES



BOARD V. MANAGEMENT – RESPONSIBILITIES

Board

- Exercise good faith, care, and loyalty
- Engage in enterprise-wide risk oversight
- Understand the strategic importance of IT to business operations and associated risk
- Ensure Management has placed qualified people in leadership roles and appropriately allocated resources to mitigate cybersecurity risk
- Understand incident response framework
- Ensure Management is enforcing an enterprise-wide cybersecurity risk management program and developed appropriate risk management policies
- Remain informed of threats, vulnerabilities, and incidents

Management

- Educate Board on cybersecurity risk; provide access to outside cybersecurity experts as appropriate
- Understand cybersecurity risk posture
- Ensure cybersecurity risk is addressed enterprise-wide
- Establish framework and infrastructure to support collaboration throughout to identify and mitigate cybersecurity risk
- Ensure allocation of sufficient human and capital resources
- Develop and implement incident response, disaster recovery, and business continuity plans and processes

WHAT ABOUT LEGAL?

- Ensure management and leadership are **aware of latest laws and regulations**
- Advise on the regulatory requirements; Support INFOSEC response to **regulatory audits**
- Consider **privilege of sensitive communications** pertaining to incidents, assessments
- Assess how information security controls may impact **individual privacy**; transparency and consumer choice best practices (the “creepy” factor)
- Ensure adequate contractual rights with vendors (downstreaming, audit, etc...)
- Protect IT and Trademark with **appropriate safeguards**

SECURITY AUDITS

- Consider **third-party consultants** to assist with needed cyber program improvements
 - Consider privilege
 - If nothing else, serves as external validation
- Audits can evaluate and test:
 - **Encryption**: Consider deploying encryption for any personal information (in transit and at rest). You will also want to understand remote connections to company systems and consider whether those connections need to be more secure

SECURITY AUDITS (CONT.)

- **Patch Management:** Confirm your patch management program is timely testing and deploying patches to software and systems
- **Asset Management/Diagram:** Identify all end points, mobile devices and other systems and devices that access your network and environment relevant to your plan
- **Multi-Factor Authentication:** Consider requiring MFA for any end points or systems that access the corporate domain related to your plan and other relevant systems, including cloud systems

SECURITY AUDITS (CONT.)

- **Access Controls:** Review identity and access management controls and policies
- **End Point Protection:** Confirm a good EDR/XDR tool has been deployed on all relevant servers, workstations and other end points
- **Backup:** Confirm important systems and data are backed up, and test the backups and confirm they can be timely recovered and implemented
- **Logs:** Confirm system, application, database, EDR, and other logs are captured, stored, and reviewed. Review log samples to confirm that logs capture necessary information

CYBERSECURITY AS A COMPETITIVE DIFFERENTIATOR



THE VALUE PROPOSITION OF CYBERSECURITY

- Good cybersecurity is a **competitive differentiator**
- The **business case for proactive cybersecurity** planning:
 - Selling point to customers and clients
 - Inspires public trust and confidence in your company
 - Avoid financial and reputational consequences of a cyberattack
 - Means fewer resources on vendor assessments



MESSAGING CYBERSECURITY TO BUSINESS STAKEHOLDERS

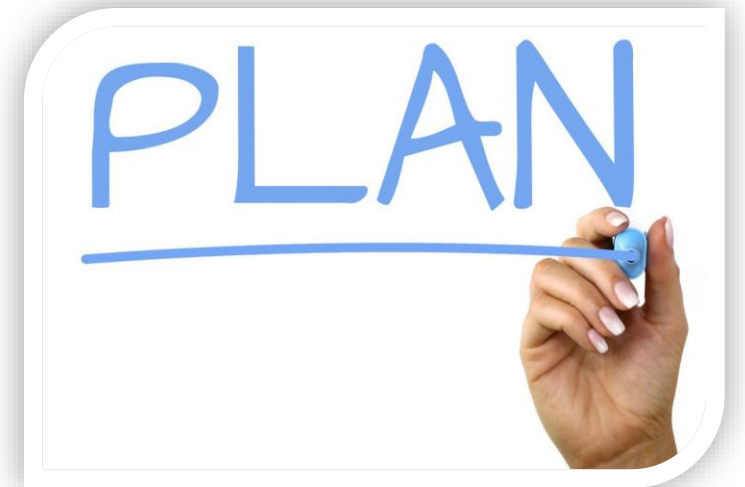
- Treating cybersecurity as **a serious business issue** (and not just an IT issue)
- Setting **realistic expectations** for a cybersecurity program—*i.e.*, risk mitigation strategy rather than a “bullet-proof vest”
- Framing incident response and remediation activities as a “**value-add**” or **investment** following a cyber-incident
- Explaining that cybersecurity is **not a one-time effort**; a successful cybersecurity program requires ongoing monitoring and implementation

BEST PRACTICES FOR INCIDENT RESPONSE

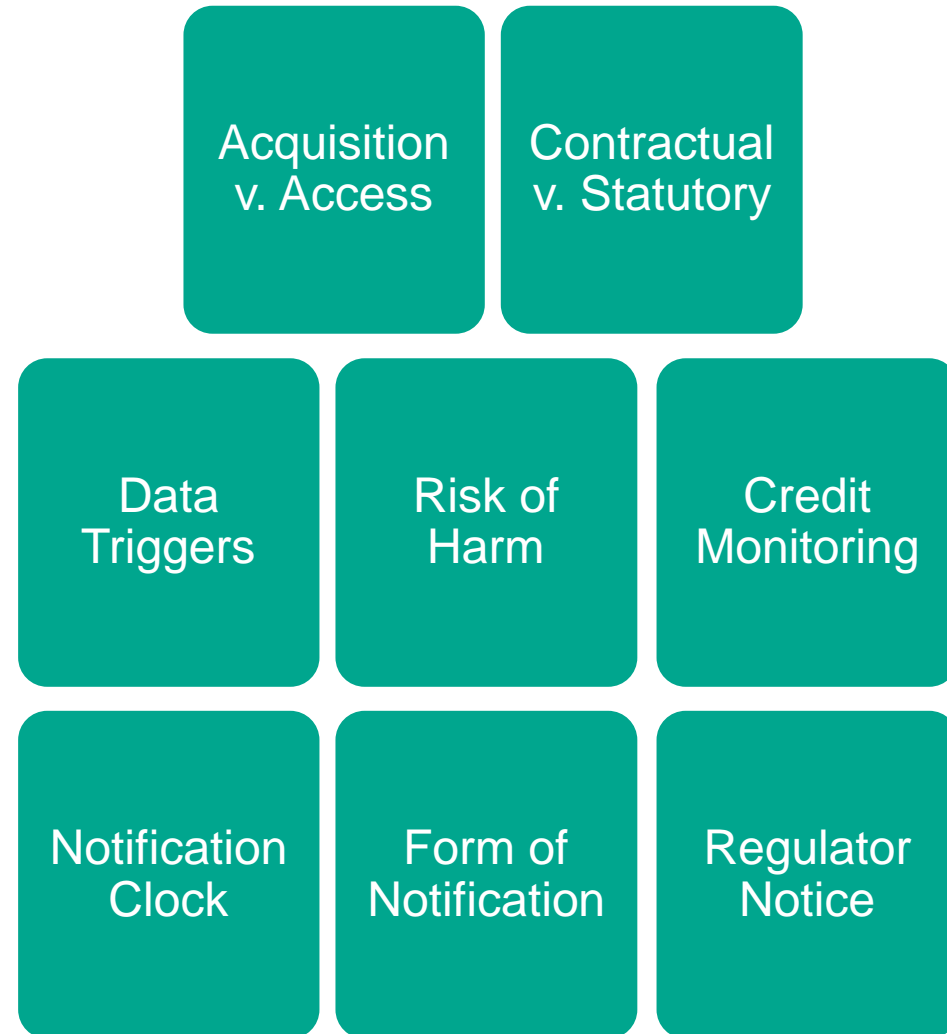


BREACH RESPONSE PREPARATION

- Proper Planning is critical:
 - Step 1: Have a Plan
 - Who is in charge?
 - Who are your external resources?
 - Step 2: Test the plan
 - Often overlooked, but infinitely valuable
 - Step 3: Insurance
 - Market is hardening
 - Step 4: Know what your contracts say



BREACH NOTIFICATION CONSIDERATIONS



COMMON CHALLENGES AND ISSUES

- Cultural, political or bureaucratic barriers to quick and efficient decision-making and delegating authority
- Identifying the appropriate decision-makers and stakeholders in a moment of crisis
- Understanding the scope of impacted data
- Determining who has ownership, stewardship, or other legal responsibility for the impacted data (or the systems where the data is stored/hosted)
- Controlling internal and external messaging
- Engaging appropriate third parties in a timely fashion



QUESTIONS / THANK YOU

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery* (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.

*For a complete list of McDermott entities visit mwe.com/legalnotices.

©2020 McDermott Will & Emery. All rights reserved. Any use of these materials including reproduction, modification, distribution or republication, without the prior written consent of McDermott is strictly prohibited. This may be considered attorney advertising. Prior results do not guarantee a similar outcome.

