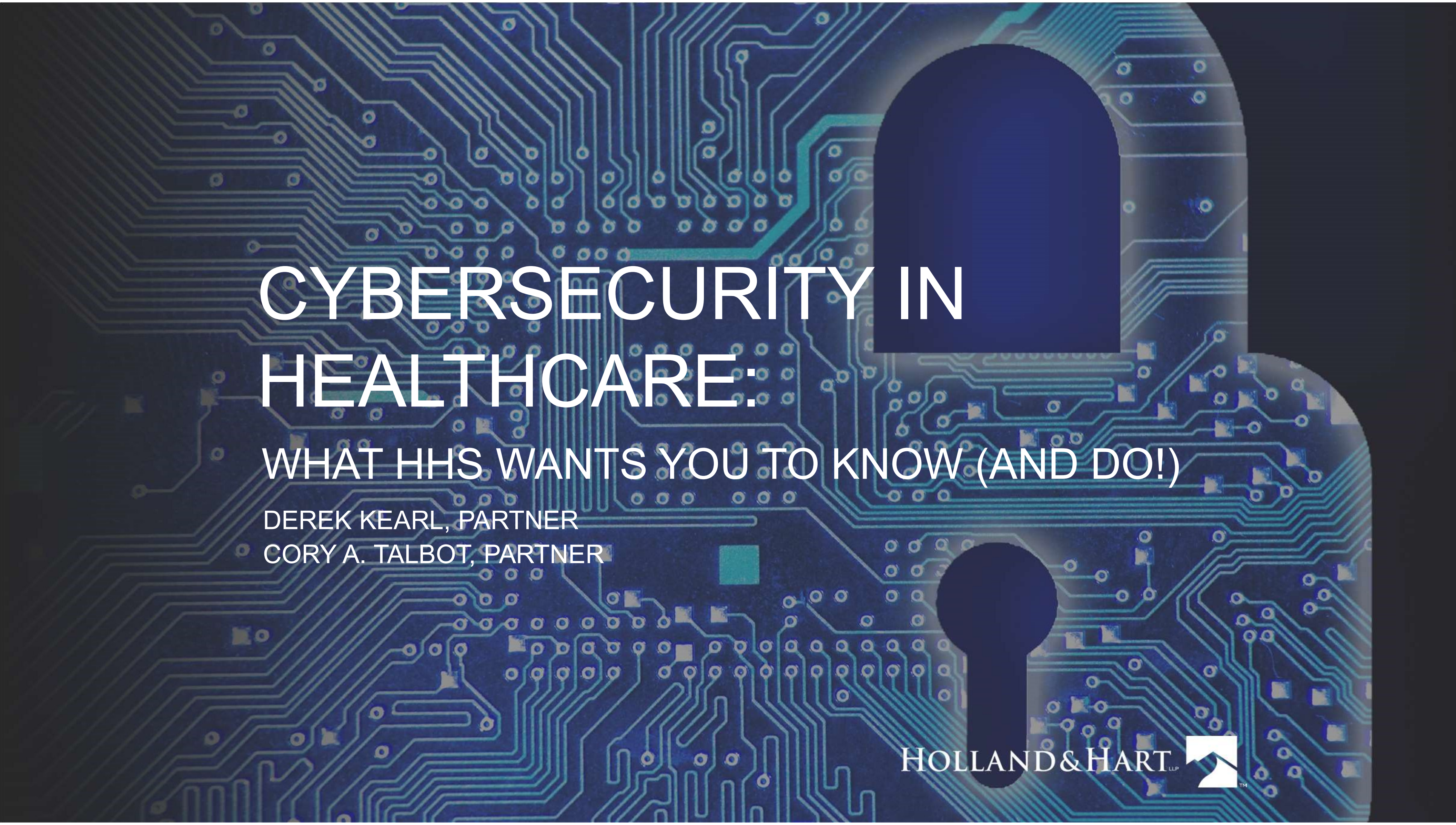


CYBERSECURITY IN HEALTHCARE:

WHAT HHS WANTS YOU TO KNOW (AND DO!)

DEREK KEARL, PARTNER
CORY A. TALBOT, PARTNER

HOLLAND&HART LLP

INTRODUCTION

DEREK KEARL
jdkearl@hollandhart.com
www.linkedin.com/in/derekkearl
801.799.5857
www.hhhealthlawblog.com

CORY A. TALBOT
catalbot@hollandhart.com
www.linkedin.com/in/corytalbot
801.799.5971
www.hhhealthlawblog.com

AGENDA

Overview of the HHS' New Cybersecurity Guidance

Description of Most Current and Common Cybersecurity Threats – and How to Address Them

Discussion of Recommended Cybersecurity Practices

HHS HEALTH INDUSTRY CYBERSECURITY PRACTICES

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

- On December 28, 2018, the Department of Health and Human Services (“HHS”) released a publication called the “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients” (“HICP”)
  - Industry-led effort
  - Response to Cybersecurity Act of 2015 mandate to develop practical cybersecurity guidelines, best practices, procedures, and processes to cost-effectively reduce cybersecurity risks for the healthcare industry
  - Product of a two-year, public-private partnership by over 150 cybersecurity and healthcare experts from industry and government
  - Aim to provide cybersecurity best practices for vast, diverse industry sector to improve the security and safety of patients and cost-effectively reduce risks

HHS HEALTH INDUSTRY CYBERSECURITY PRACTICES

"Cyberattacks are an increasing threat across all critical infrastructure sectors. For the health sector, cyberattacks are especially concerning because these attacks can directly threaten not just the security of our systems and information but also the health and safety of American patients. We are under constant cyberattack in the health sector, and no organization can escape that reality." Eric Hargan, Deputy Secretary of HHS.

HHS HEALTH INDUSTRY CYBERSECURITY PRACTICES

4 in 5 physicians have suffered some type of cybersecurity attack.

The impact can be severe:

- "58% of malware attack victims are small businesses."
- "In 2017, cyber-attacks cost small and medium-sized businesses an average of $2.2 million."
- "60% of small businesses go out of business within six months of an attack."
- "90% of small businesses do not use any data protection at all for company and customer information."

HHS HEALTH INDUSTRY CYBERSECURITY PRACTICES

HICP: Managing Threats and Protecting Patients: Overview of cybersecurity threats that affect the healthcare industry

Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations

Four Volume Publication

(****Cybersecurity Practices Assessments Toolkit:** Under Development)

Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations

Resources and Templates: Additional resources and references

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Most Current and Common Cybersecurity Threats

- Email Phishing Attacks
- Ransomware Attacks
- Loss or Theft of Equipment or Data
- Insider, Accidental, or Intentional Data Loss
- Attacks Against Connected Medical Devices

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Threat: Email Phishing Attack

- Description
  - Email phishing is an attempt to trick you into giving out information using email.
  - Appears to come from a legitimate source
  - Includes active link or file.
  - Clicking link or file takes user to website that solicits sensitive data or may infect the computer
- Real-World Scenario
  - Employees receive a fraudulent email from a cyber-attacker, disguised as an IT support person from your patient billing company.
  - Email instructs employees to click on a link to change billing software passwords.
  - Employee clicks on link, is directed to fake login page, which collects employees login credentials.
  - Attacker uses credentials to access financial and patient data.
- Impact
  - Pediatrician learns that an attacker stole patient data using a phishing attack and used it in an identity theft crime.

Threat Quick Tips: Email Phishing Attack

- What to Ask?
  - Do you know the sender?
  - Spending/grammatical errors?
  - Hover over link to see URL destination?
  - When in doubt, do NOT click links/open attachments.
  - Processes for reporting suspicious emails?
- When to Ask?
  - The best time to familiarize oneself with policies for reporting suspicious email is beginning of employment.
  - Verify before opening suspicious email.
- Who to Ask?
  - Check with colleagues to find out if they received similar phishy email
  - Seek guidance from IT security support team or similar point of contact.

Threat: Email Phishing Attack

Vulnerabilities

- Lack of IT resources for managing suspicious email

Impact

- Loss of reputation in the community (referrals dry up, patients leave)
- Stolen credentials used to access sensitive data

Practices to Consider

- Be suspicious of emails from unknown senders that request sensitive data (PHI or PII), or emails that include a call to action or stress urgency

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Threat: Loss or Theft of Equipment or Data

- Description
  - Mobile devices – laptops, tablets, smartphones, thumb drives, etc. – are lost or stolen daily, sometimes ending up in the hands of hackers.
  - In just the first eight months of 2018, OCR received reports of nearly 200 theft cases affecting over two million individuals.
  - The loss of a device that is not appropriately safeguarded or password protected may result in unauthorized or illegal access, dissemination, and use of sensitive data.
  - Even if the device is recovered, the data may have been erased and lost. Loss or malicious use of data may disrupt business, compromise patient safety, and even require notification to patients, regulatory agencies, and/or the media.
- Real-World Scenario
  - A physician stops at a coffee shop and uses public Wi-Fi to review radiology reports.
  - As the physician leaves the table momentarily to pick up his coffee, a thief steals the laptop.
  - The doctor returns to the table to find the laptop is gone.
- Impact
  - Losing sensitive data may lead to patient identity theft.
  - With thousands of records potentially stolen, the physician’s reputation could be at stake if patient records make it to the dark web for sale.
  - OCR fines.

Threat Quick Tips: Loss of Equipment or Data

– What to Ask?

- Make sure you know your organization’s policy on removing equipment from the workplace by asking:
  - Can I travel with my equipment?
  - Can I take my equipment offsite to work remotely?
  - Are USB or other portable storage devices allowed?
  - Is the information on my computer or storage device encrypted?
  - Is there a secure virtual private network (VPN) that I can use, along with secure, password-protected Wi-Fi, to log into the network and work?

– When to Ask?

- As soon as you realize that your device or equipment has been stolen or misplaced, notify your supervisor and IT security professional immediately so appropriate measures can be taken to safeguard the data on your device or equipment.

– Who to Ask?

- Notify your IT security support staff or similar point of contact when a work device or equipment has been misplaced, lost, or stolen.

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Threat: Loss or Theft of Equipment or Data

- Vulnerabilities
  - Lack of asset inventory and control
  - Lack of encryption
  - Lack of physical security practices
  - Lack of simple safeguards such as computer cable locks to secure devices in the office
  - Lack of awareness that theft of IT assets from the office accounts for nearly as much as from cars
  - Lack of effective vendor security management, including controls to protect equipment or sensitive data
  - Lack of "End-of-Service" process to clear sensitive data before IT assets are discarded or transferred

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Threat: Loss or Theft of Equipment or Data

- Impact
  - Inappropriate access to or loss of sensitive patient information
  - Theft or loss of unencrypted PHI or PII
  - Lost productivity
  - Damage to reputation

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Threat: Loss or Theft of Equipment or Data

- Practices to Consider
  - Encrypt sensitive data, especially when transmitting data to other devices or organizations
  - Implement proven and tested data backups, with proven and tested restoration of data
  - Acquire and use data loss prevention tools
  - Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices
  - Promptly report loss/theft to designated company individuals to terminate access to the device and/or network
  - Maintain a complete, accurate, and current asset inventory
  - Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device
  - Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold

HICP: MANAGING THREATS AND PROTECTING PATIENTS

Ten practices to mitigate cybersecurity threats

1 Email Protection Systems

2 Endpoint Protection Systems

3 Access Management

4 Data Protection and Loss Prevention

5 Asset Management

6 Network Management

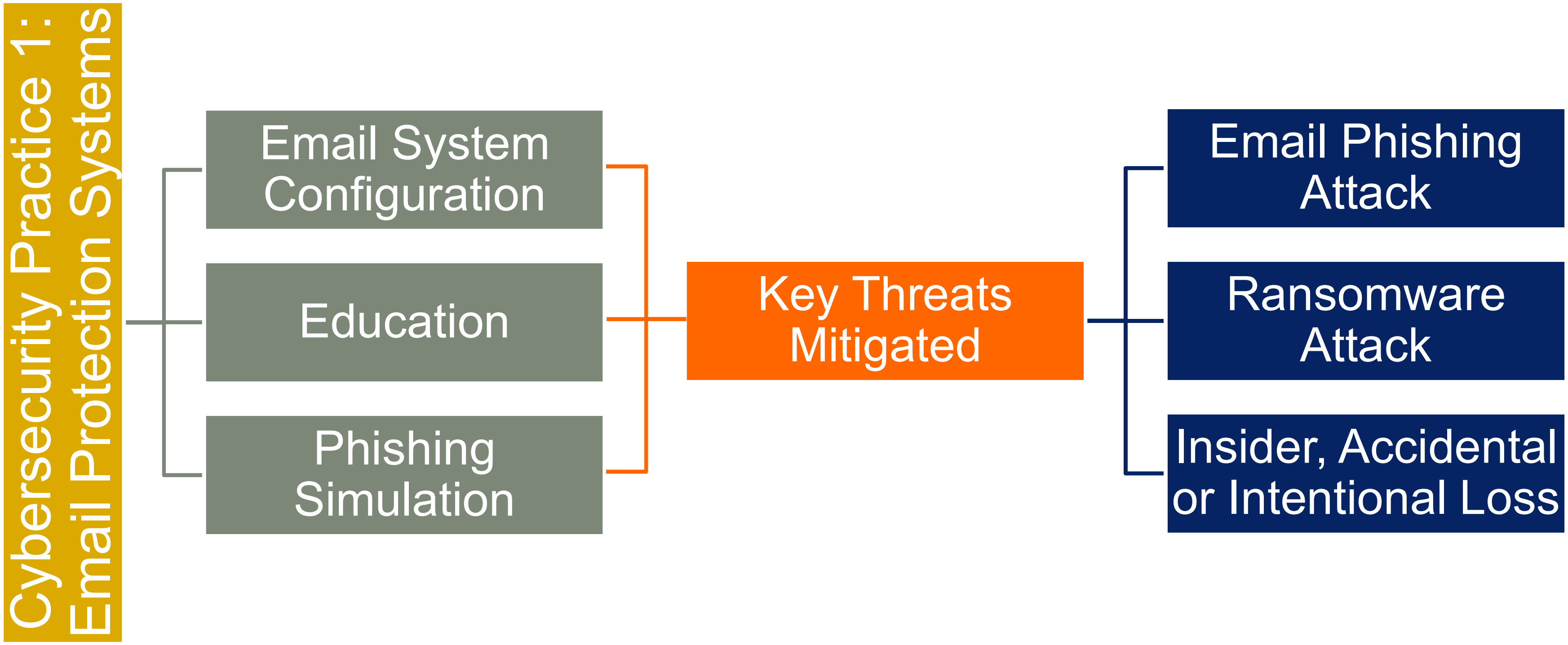
7 Vulnerability Management

8 Incident Response

9 Medical Device Security

10 Cybersecurity Policies

SUB-PRACTICES FOR SMALL ORGANIZATIONS



Cybersecurity Practice 1:
Email Protection Systems

Email System Configuration

Education

Phishing Simulation

Key Threats Mitigated

Email Phishing Attack

Ransomware Attack

Insider, Accidental or Intentional Loss

SUB-PRACTICES FOR MEDIUM AND LARGE ORGANIZATIONS

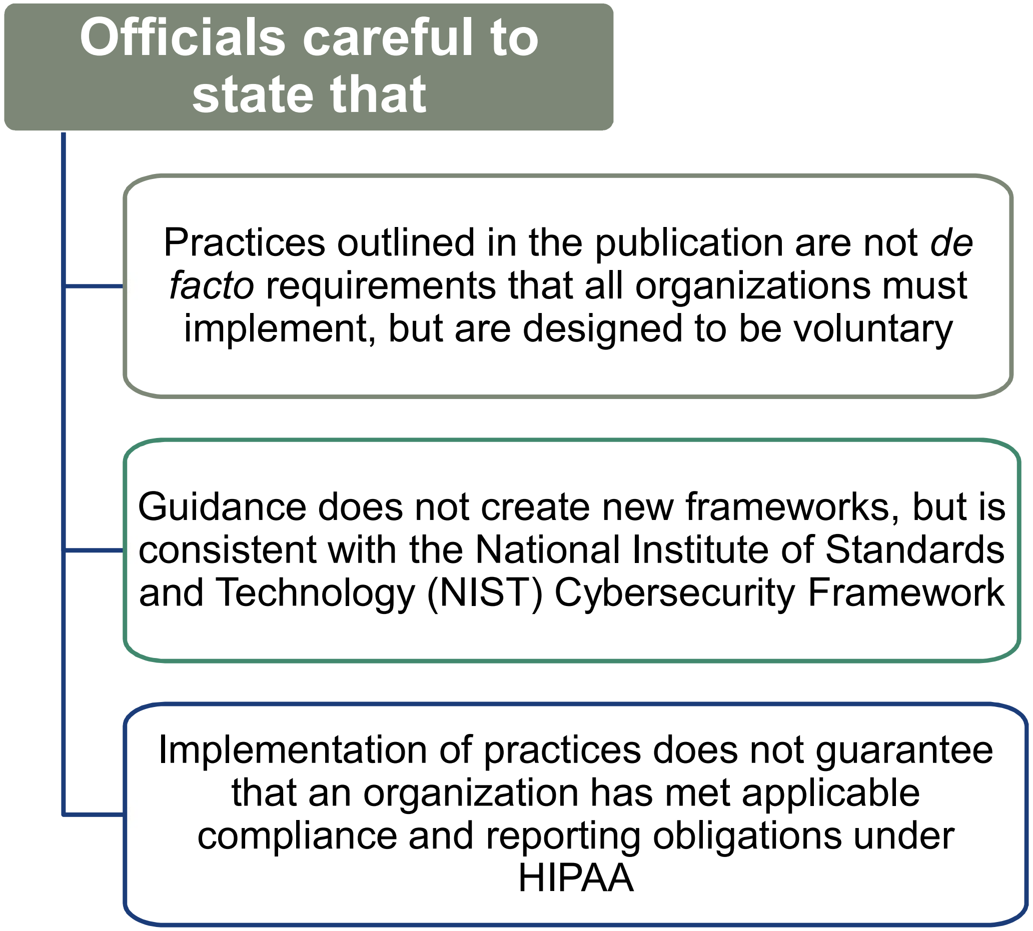
Cybersecurity Practice 1: E-mail Protection Systems	
Data That May Be Affected	• Passwords, PHI
Medium Sub-Practices	• Basic E-mail Protection Controls • Multifactor Authentication for Remote Access • E-mail Encryption • Workforce Education
Large Sub-Practices	• Advanced and Next-Generation Tooling • Digital Signatures • Analytics Driven Education
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Insider, Accidental or Intentional Data Loss

CYBERSECURITY PRACTICE 10 – CYBERSECURITY POLICIES

Effective Policies to Mitigate the Risk of Cybersecurity Attack

Policy Name	Description
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices and setting and establishing policy.
Education and Awareness	Describe the mechanisms by which the workforce will be trained on cybersecurity practices, threats, and mitigations.
Acceptable Use / E-mail Use	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how e-mail will be used to complete work.
Data Classification	Describe how data will be classified, with usage parameters for each classification. This classification should be in line with Cybersecurity Practice #4.
Personal Devices	Describe the organization's position on usage of personal devices, also referred to as bring your own device (BYOD). If usage of personal devices is permitted, describe the expectations for how the devices will be managed.
Laptop, Portable Device, and Remote Use	Describe the policies that relate to mobile device security and how these devices may be used in a remote setting.
Incident Reporting and Checklist	Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.

IMPACT OF HICP?



Officials careful to state that

Practices outlined in the publication are not *de facto* requirements that all organizations must implement, but are designed to be voluntary

Guidance does not create new frameworks, but is consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework

Implementation of practices does not guarantee that an organization has met applicable compliance and reporting obligations under HIPAA

But, the thorough and detailed nature of the guidance, and the fact that they are the result of a consensus-based, industry and government-led process, makes the HICP guidance an important guidepost

KEY TAKEAWAYS

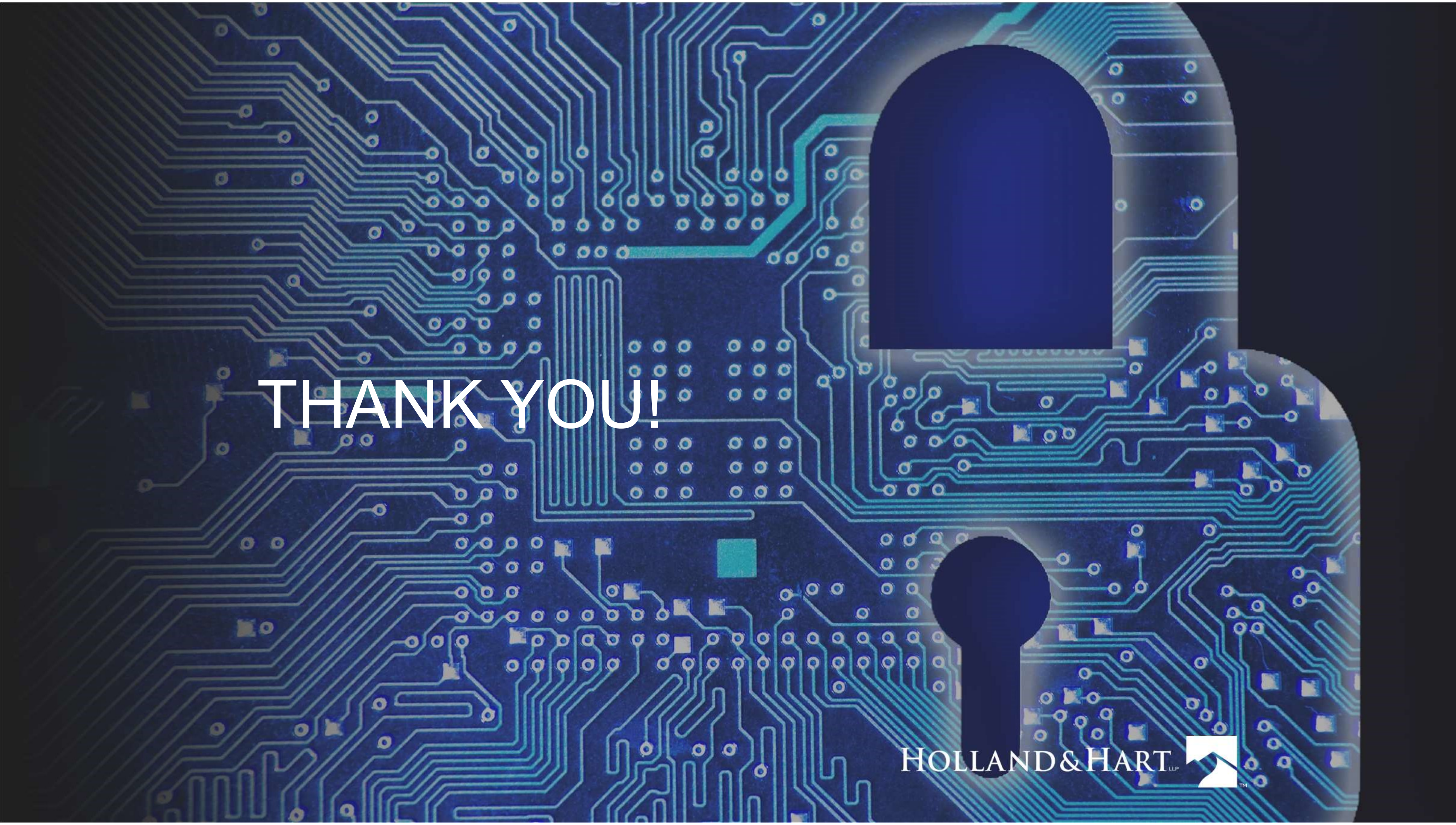
DO

- Develop and implement a cybersecurity compliance program.
- Evaluate and benchmark cybersecurity capabilities within your organization.
- Examine cybersecurity threats to your organization.
- Prioritize actions and investments to improve cybersecurity within your organization.
- Share knowledge and best practices across your organization.
- Tailor cybersecurity practices to your unique needs.

QUESTIONS OR COMMENTS?

DEREK KEARL
jdkearl@hollandhart.com
www.linkedin.com/in/derekkearl
801.799.5857
www.hhhealthlawblog.com

CORY TALBOT
catalbot@hollandhart.com
www.linkedin.com/in/corytalbot
801.799.5971
www.hhhealthlawblog.com



THANK YOU!