RISK IN HEALTHCARE

Leading edge security and risk management practices

September 27, 2018
Presenters

Anthony Catalano
Director
• Healthcare Virtual CISO
• CISSP, PCI QSA, HITRUST CCSFP

Greg Vetter
Principal
National HIPAA and HITRUST service Leader
By the end of this webcast you will be able to

- Identify practical information protection measures implemented at the most sophisticated health systems
- Understand the concept of a comprehensive business process risk assessment
- Describe risk management trends for 2019
- Understand advanced employee education, training and testing
RISK MANAGEMENT

Practical information protection measures implemented at the most sophisticated health systems
Key Takeaways:

• Approximately 63 percent of healthcare breaches were caused by criminal or malicious activity

• Few companies have more information, at a greater market value, on their customers than those in healthcare.

• Healthcare has improved its security posture in recent years and is generally average when compared to other industries.
  – However, the value of healthcare data remains relatively high
  – Healthcare organizations often pair healthcare and payment or financial data together.
Evolution of cybersecurity risk management

**Transactional**
- Risk is “Bad”
- Focus on identifying and improving controls around risk
- Risk is not integrated or managed across the entire organization.
- Compliance Issues addressed Separately.

**Integrated**
- Risk is bad–focus is on transferring risk
- Risk is an expense–focus is on managing risk

**Strategic**
- Risk is uncertainty–focus is on optimization and ability to respond & recover.

**Advanced risk management**
- Proactive about preventing and managing risk
- More collaboration
- Where is my next best security dollar spent?

**Traditional risk management**
- Risk is “Bad”
- Focus on identifying and improving controls around risk
- Risk is not integrated or managed across the entire organization.
- Compliance Issues addressed Separately.
Impacts

- Direct costs to recover from a breach
- Regulatory fines
- Privacy protection costs
- Theft of intellectual property
- Decreased earning potential
- System downtime and lost productivity
- Existing customers lose confidence
- Reduction in new customers
- Employee moral or retention

*Some of these impacts can be transferred via insurance, some cannot!*
Governance

• Sophisticated Health systems have steering committees.

• Represent a holistic approach to cyber security that involves business owners, executives, and operations teams to help promote a culture of security.

• Decisions cannot be made in a vacuum, and everyone has to agree what the mission of the team is.
### Six pillars of cybersecurity – measurement is key!

<table>
<thead>
<tr>
<th>1. Security governance</th>
<th>2. Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>This initiative consists of formally establishing direction, management, oversight, and accountability for security initiatives. Strong governance is the foundation for ensuring security projects address risks, align with business objectives, and are completed effectively and efficiently.</td>
<td>If users are properly trained, they can be the first line of defense against some of the most common and successful attacks. A strong training program builds a culture of awareness and instills accountability at all levels of the organization.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Detection &amp; incident preparedness</th>
<th>4. Technical hardening &amp; testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>When security incidents occur, the goal is to return the business to normal operations as quickly as possible by limiting damage, business impact, recovery time, and costs. To do so, a combination of tools, monitoring, IR procedures, and crisis plans are essential.</td>
<td>Aligning network and system components with security best practices provides visibility into exposures, and promotes consistency and efficiency across the environment. Regular testing provides metrics and validation to ensure controls are effective.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. Data protection</th>
<th>6. Third party risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Since data is what attackers seek, it is important to ensure it is protected from both accidental and intentional misuse and disclosure. To do so, the company must identify what kind of data lives in the environment, establish requirements for protecting that data, and implement policies and technical safeguards.</td>
<td>Collaborating with third parties can introduce known and unknown risks into an environment. Standardizing procedures for these partnerships can reduce risk, optimize resources, and ensure the responsible parties are upholding all compliance and security obligations.</td>
</tr>
</tbody>
</table>
# widgets inc corporation – it/is key risks indicators

<table>
<thead>
<tr>
<th>Cyber Risk Management &amp; Oversight</th>
<th>Risk Appetite</th>
<th>Aug-17</th>
<th>Jul-17</th>
<th>Jun-17</th>
<th>May-17</th>
<th>Apr-17</th>
<th>Mar-17</th>
<th>Feb-17</th>
<th>Jan-17</th>
<th>Dec-16</th>
<th>Nov-16</th>
<th>Oct-16</th>
<th>Sep-16</th>
<th>KRI TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Rate % of Mock Phishing Campaign</td>
<td>&lt; 10%</td>
<td>&gt;10%</td>
<td>&lt;15%</td>
<td>&gt;15%</td>
<td>8%</td>
<td>2%</td>
<td>n/a</td>
<td>n/a</td>
<td>17%</td>
<td>n/a</td>
<td>n/a</td>
<td>14%</td>
<td>4%</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Intelligence &amp; Collaboration</th>
<th>Risk Appetite</th>
<th>Aug-17</th>
<th>Jul-17</th>
<th>Jun-17</th>
<th>May-17</th>
<th>Apr-17</th>
<th>Mar-17</th>
<th>Feb-17</th>
<th>Jan-17</th>
<th>Dec-16</th>
<th>Nov-16</th>
<th>Oct-16</th>
<th>Sep-16</th>
<th>KRI TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threat Level</td>
<td>&lt; 1</td>
<td>≥2</td>
<td>≥3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity Controls</th>
<th>Risk Appetite</th>
<th>Aug-17</th>
<th>Jul-17</th>
<th>Jun-17</th>
<th>May-17</th>
<th>Apr-17</th>
<th>Mar-17</th>
<th>Feb-17</th>
<th>Jan-17</th>
<th>Dec-16</th>
<th>Nov-16</th>
<th>Oct-16</th>
<th>Sep-16</th>
<th>KRI TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Score of Patches Not Applied &gt;90 Days</td>
<td>&lt; 100k</td>
<td>&gt;100k</td>
<td>&lt;150k</td>
<td>&gt;150k</td>
<td>162k</td>
<td>375k</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>INCREASING</td>
</tr>
<tr>
<td>Risk Score of Unsupported Systems</td>
<td>&lt; 15</td>
<td>&gt;15</td>
<td>&lt;20</td>
<td>&gt;20</td>
<td>16</td>
<td>16</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>STABLE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Third Party Security Management</th>
<th>Risk Appetite</th>
<th>Aug-17</th>
<th>Jul-17</th>
<th>Jun-17</th>
<th>May-17</th>
<th>Apr-17</th>
<th>Mar-17</th>
<th>Feb-17</th>
<th>Jan-17</th>
<th>Dec-16</th>
<th>Nov-16</th>
<th>Oct-16</th>
<th>Sep-16</th>
<th>KRI TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of Third Party Reviews Not Completed</td>
<td>&lt; 10%</td>
<td>&gt;10%</td>
<td>&lt;25%</td>
<td>&gt;25%</td>
<td>34%</td>
<td>32%</td>
<td>14%</td>
<td>28%</td>
<td>6%</td>
<td>3%</td>
<td>16%</td>
<td>18%</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td># of Third Party Control Requirements Open &gt; 30 days</td>
<td>≤2</td>
<td>&gt;2</td>
<td>≤5</td>
<td>&gt;5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber Incident Management and Resilience</th>
<th>Risk Appetite</th>
<th>Aug-17</th>
<th>Jul-17</th>
<th>Jun-17</th>
<th>May-17</th>
<th>Apr-17</th>
<th>Mar-17</th>
<th>Feb-17</th>
<th>Jan-17</th>
<th>Dec-16</th>
<th>Nov-16</th>
<th>Oct-16</th>
<th>Sep-16</th>
<th>KRI TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Open vs Closed Incidents</td>
<td>≤2</td>
<td>&gt;2</td>
<td>≤5</td>
<td>&gt;5</td>
<td>0/7</td>
<td>2/10</td>
<td>0/5</td>
<td>0/6</td>
<td>0/2</td>
<td>0/15</td>
<td>0/8</td>
<td>0/11</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Security Compliance Risk

• The HIPAA Security Rule Big Ticket Items:
  – Current and accurate security polices
  – Complete and accurate risk analysis
  – Periodic risk assessments
  – Breach response timeliness and thoroughness
Basics of the Risk Analysis

Inventory
- Assets and processes related to ePHI

Threat
- What could expose or damage ePHI

Controls
- How do we protect against the threats

Vulnerabilities
- What risks remain after we apply controls

Corrective Actions
- How will we minimize the risks with new controls etc.

New systems, sites, changes

New controls, vulnerabilities, and actions

Timely Update
SECURITY IMPLEMENTATION

Practical information protection measures implemented at the most sophisticated health systems
NIST Cyber Security Framework mapping and maturity progression

NIST CSF measured security progress

- **Identify**
  - ID.BE-4: Dependencies and critical functions for delivery of critical services are established
  - ID.BE-5: Resilience requirements to support delivery of critical services are established
- **Protect**
  - Maintenance (PR.MA)
  - Protective Technologies (PR.PT)
- **Detect**
  - Detective abilities can be improved and this should remain a focus for the organization. Specifically:
    - Anomalies and Events (DE.AE)
    - Security and Continuous Monitoring (DE.CM)
    - Detection Processes (DE.CP)
  - The organization should seek to improve logging and monitoring capability around critical business processes.
- **Respond**
  - Most Response capability is repeatable – to achieve an adaptive state (4) the organization will need to incorporate the processes with lessons learned and embed with company culture, with proactive collaboration.
- **Recover**
  - Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events
  - The Organization should move to improve overall recovery capability. Implement yearly or semiannual IR tabletop sessions with both staff and executive teams.
### NIST CSF tier levels

<table>
<thead>
<tr>
<th>Tier 1</th>
<th>Partial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management is ad hoc, with limited awareness of risks and no collaboration with others.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 2</th>
<th>Risk informed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management process and programs are in place but are not integrated enterprise wide. Collaboration is understood, but the organization lacks formal capabilities.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 3</th>
<th>Repeatable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal policies for risk management processes and programs are in place enterprise wide, with partial external collaboration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 4</th>
<th>Adaptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management processes and programs are based on lessons learned and embedded in culture, with proactive collaboration.</td>
<td></td>
</tr>
</tbody>
</table>
Vendor risk management

- Development of due diligence questionnaire
  - Questionnaire and control assessment based on NIST 800-53, Shared Assessment Program and/or CIS Frameworks
  - Cloud and non-cloud vendors

- Development of weighted risk criteria
  - Cloud vs non-cloud vendors

- Distribution of vendor questionnaires via RSM Vendor Management Portal to 20-30 high risk application vendors
  - Questionnaire and control assessment based on NIST 800-53, Shared Assessment Program and/or CIS Frameworks

- All information normalized and incorporated back into the risk management program.
Why is vendor risk management important?

- It is not enough to secure PHI within your own organization; you are responsible for third-party associates as well.

- Third party associates, defined as “business associates” or BAs, can include outside consultants (such as claims processing administrators) as well as independent software providers (such as physician transcription services).

$1.55 million settlement underscores the importance of executing HIPAA business associate agreements
Red team/blue team = purple team

- Red team and blue team exercises not as valuable as they used to be.
- The purpose of a purple team assessment is to evaluate the effectiveness of the security controls an organization has deployed within its environment.
- This assessment focuses on the ability of the organization to block external and internal attacks, and in the event a breach occurs, detect malicious activity within the infrastructure.
Purple team output

- Tactical recommendation plan
  - Resolve Symantec alerts
  - Configure LogRhythm alerts on windows event logs

- Strategic recommendation plan
  - Regularly test different business cases
  - Refine logging and monitoring capabilities
Keys to a successful purple team

- Management direction for collaboration among the team members
- Defined team objectives focused on the improvement of skills and controls
- Sufficient time for debrief sessions:
  - to explore the attack techniques used to provide the Blue Team with insight – methodologies and tools used
  - To explore the defenses deployed to allow the Red Team to craft new attacks (the attackers are always learning!)
BUSINESS PROCESS RISK ASSESSMENT

Understanding the concept of a comprehensive business process risk assessment
Integrated cyber risk management – business case for cyber risk

- Traditional cybersecurity risk evaluation lacks context
- Risks rated by likelihood and impact.
- Too broad, does not drive monetarily responsible decisions.

By quantifying exposure per process, we can start to understand where the greatest risks lie, and spend accordingly.

- $78M Total risk exposure based on processes reviewed
- 48% Controls were in place
- $8M Risk transferred through Cyber Liability Insurance
- 10% Of total risk protected through Cyber Liability Insurance
- 78% Reduction in risk is possible with proposed mitigations
- $17.4M Total risk exposure remaining after mitigation
Business process risk assessment

- The business process risk assessment is used to determine the risk of potential financial losses to which each business process exposes the organization.

- This assessment includes identifying people, processes, and technology (including third parties) involved in the in-scope processes and the associated risks posed to the organization.

- In addition to monetizing risk, this assessment facilitates the development of a roadmap/framework to improve the corporate security program.

**BUSINESS PROCESS RISK ASSESSMENT**

<table>
<thead>
<tr>
<th>1</th>
<th>KE DATA</th>
<th>2</th>
<th>THREATS</th>
<th>3</th>
<th>PROCESS FLOW</th>
<th>4</th>
<th>CONTROL RISK</th>
<th>5</th>
<th>RISK LEVEL</th>
<th>6</th>
<th>DOCUMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DATA TYPE</td>
<td>IMPACT X LIKELIHOOD</td>
<td>DOCUMENT &amp; VALIDATE</td>
<td>IN PLACE CONTROLS</td>
<td>CALCULATE EXPOSURE</td>
<td>BUSINESS PROCESSES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PROCESS VALUE</td>
<td>DETERMINE SPTA</td>
<td>UNKNOWN PROCESSES</td>
<td>VULNERABILITIES</td>
<td>CURRENT STATE RISK LEVEL</td>
<td>OVERALL RISK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SINGLE LOSS POTENTIAL</td>
<td>ATTACK VECTORS</td>
<td>NETWORK ARCHITECTURE</td>
<td>DETERMINE EFFECTIVENESS</td>
<td>FUTURE STATE RISK LEVELS</td>
<td>QUANTITATIVE &amp; QUALITATIVE ASSUMPTIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CONFIDENTIALITY INTEGRITY AVAILABILITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2018 RSM US LLP. All Rights Reserved.
OBSERVATIONS
The overall results show the business processes assessed at Widgets INC have a combined exposure of more than $78M, and an overall low average risk rating. The primary factors contributing to the risk ratings are:

- The Widgets INC cardholder data (CHD) despite tokenization being in place
- Credit card transactions are accepted within Widgets INC application without the use of outsourcing technology
- Claims data is sent to customers via insecure email
- Passwords length requirements do not align with the security best practices and users are also frequently using the same passwords for their domain accounts and multiple applications.
- Widgets INC does not test its external or internal applications, such as REDACTED.
- Widgets INC has difficulty monitoring compliance for Independent agents who receive CHD and personally identifiable information (PII).
- The practices used within the PCI Zone have not been extended to the rest of the organization.

$78M
Total risk exposure based on processes reviewed

48%
Controls were in place

$8M
Risk transferred through cyber liability insurance

10%
Of total risk protected through cyber liability insurance

78%
Reduction in risk is possible with proposed mitigations

$17.4M
Total risk exposure remaining after mitigation
EXECUTIVE SUMMARY
As part of an internal goal to understand how Watts Refrigeration (Watts) is performing against industry benchmarks, RSM was selected to conduct an Information Security Maturity Assessment (INFOSEC) along with Strategic and Operational (S&O) Planning. The output of those assessments allow Watts to properly understand areas of strength and opportunity for growth. In addition, RSM and Watts have used these results to collaboratively build a roadmap that can be executed during the next one-three years to achieve higher levels of maturity and ultimately reduce risk within the organization. These assessments were completed through interviews and reviews of documentation during the months of October and November 2017.

OBSERVATIONS
RSM has a strong partnership with Watts and, in addition to the work performed as part of this assessment, has performed a variety of other services that have been incorporated into the results of this assessment. Overall, it has been recognized that the security team with Watts has put substantial effort into improving the program. There have been significant investments made in tools and technology, which have led to a high percentage of mature controls being in place. However, we have found that limited operational focus outside that of necessary areas such as PCI or SOX compliance have led to a lower than expected maturity ranking of 1-Initial for the overall program, as compared to Level 2-Repetable as an average for the retail industry. The following table lists the high-level strengths and opportunities observed by RSM:
Budget trends and analysis

• IT budgets are typically three to seven percent of a company’s revenue, and security budgets are typically five to eight percent of IT spend.
  - Assumed for a mature program, when “catching up” can go up to 30 percent.
A partnership model with IT Audit

• IT Audit should have a broad knowledge of the organization’s information assets through risk assessment process

• Instead of silos, Audit and Security should actively partner to drive better outcomes

• Examples:
  − Security involvement in the annual IT audit risk assessment
  − Audit involvement in major information security capital investment decisions
Internal Audit

- **Evaluate the full cybersecurity framework, rather than cherry pick items.** This evaluation involves understanding the current state against framework characteristics, where the organization is going, and the minimum expected cybersecurity practices across the industry or business sector.

- **The initial assessment should inform further, more in-depth reviews.** It is not intended to be an exhaustive analysis requiring extensive testing. Rather, the initial assessment should drive additional risk-based cybersecurity deep dive reviews.
Collaboration is Critical

Security
- Directs/Manages the Information Security Program
- Works with client leadership to establish requirements for security program
- Identifies, communicates and provides recommendations for security risks
- Tests security controls implementation effectiveness
- Works with client leadership to define metrics

Internal Audit
- Validates adherence to security requirements
- Validates adherence to defined metrics

Operations
- Implements security controls
- Abides by policy
- Manages technical components
- Provides internal project management
HITRUST CSF to address healthcare challenges

HITRUST DESIGN =

Consistent
Efficient

Cost Reduction
Minimize Risk
What is the HITRUST CSF

The HITRUST CSF

The HITRUST (CSF) provides coverage across multiple healthcare specific standards and includes significant components from other well-respected IT security standards bodies and governance sources

• Simply put: The HITRUST CSF is a standard built upon other standards and authoritative sources relevant to the healthcare industry.
  • It harmonizes existing controls and requirements from standards, regulations, business and third party requirements applicable to healthcare
  • It incorporates both compliance and risk management principles
  • It defines a process to effectively and efficiently evaluate compliance and security risk, which includes the HIPAA Final Rule Requirements
  • Supports CSF certification
What are Control Categories, Control Objectives & Implementation Requirements

- **Control Categories**
  - High level categories initially based on ISO27001 & 27002
  - **Example**: 01:0 Access Control

- **Control Objectives (Objective Names)**
  - A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process
  - **Example**: to prevent unauthorized users access, and compromise or theft of information and information assets. (01.03 User Responsibilities)

- **Implementation Requirements**
  - The prescriptive statements in support of the establishment and maintenance of a control to meet the business, security and regulatory goals of the organization
  - **Example**: Password management policies shall be developed, documented, adopted and communicated to all users to address the need to …. (01.f Password Use – Level 1 )
Working with HITRUST can involve several different approaches and steps.

- **SOC 2 + HITRUST**: Assist client with aligning Trust Services Principles and Criteria to the HITRUST CSF.
- **Self Assessment**: Assist client with completing HITRUST self assessment.
- **Framework Implementation**: Assist client with implementing HITRUST as a framework for their environment.
- **Validated Assessment**: Act as a 3rd party assessor to validate a client’s HITRUST implementation.
- **Validated & Certified Assessment**: Act as a 3rd party assessor to validate a client’s HITRUST implementation and submits review to HITRUST.
The impact of GDPR

• Unlike HIPAA, which has a maximum fine penalty of $1.5 million per year for violations of an identical provision, GDPR fines can cost up to $24 million or four percent of an organization's annual global revenue - whichever is higher.

• GDPR has the potential to be massively impactful business processes across all sectors, globally. In fact, experts agree GDPR could be much more significant than HIPAA, not only punitively, but also in scope.
Other impacts

- Consent – do you have explicit consent from individuals for the data you hold about them?
  Under the new rules the requirements have been tightened significantly. Requesting consent from a consumer to process their personal data must be unambiguous.

- New responsibilities - are you a data processor or data controller responsible for processing personal data?
  Under the GDPR, data processors will have greater legal liability and are required to maintain records of personal data and processing activities. There are also further obligations on controllers to ensure that any third-party contractors also comply with the GDPR, e.g. cloud hosting or outsourcing.

- Mandatory breach notification – would you be able to notify a data protection supervisory authority of a data breach within 72 hours?
  You will need internal processes that allow you to report and manage communications with affected consumers quickly and accurately.

- Data protection officers – do you conduct large scale systematic monitoring (including employee data) or process large amounts of sensitive personal data?
  Where large scale processing of data is evident a dedicated Data Protection Officer needs to be appointed.
Where to start?

- **Is your entity located in the EU?**
  - YES → GDPR applies
  - NO →
    - **Is the Data Subject a resident of or currently travelling in the EU?**
      - YES → GDPR applies
      - NO →
        - **Does the processing relate to commercial activity?**
          - YES → GDPR applies
          - NO →
            - **Does the processing relate to monitoring behavior?**
              - YES → GDPR applies
              - NO → GDPR does not apply

© 2018 RSM US LLP. All Rights Reserved.
Data classification

• Organizations will be forced to classify their data, something all organizations should do anyway, simply because data classification helps you understand your assets, where they are located, and which are worth protecting at all costs.

• Unlike HIPAA, which has settled on a definition for electronic protected health information, GDPR remains vague at this point, but we can expect the scope of personal data protection to be big.

• We’ll likely see a data set that will include photos, IP addresses, social media posts, cookies that your browser may have dropped from an endpoint, individual likenesses, biometrics and more.
SECURITY AWARENESS TRAINING

Practical information protection measures implemented at the most sophisticated health systems
Security awareness

- Understand advanced employee education, training and testing
  - Phishing
  - Targeted training
Employees can be the weakest link or the first line of defense...

- Invest in training your employees.
- RSM recommends quarterly training and testing.
- **Free** tool to help organizations with this initiative.
Resiliency

- According to a recent report by PhishMe.
- **Resiliency = Number of reported/number of susceptible.**
  - Lower susceptibility + higher reporting = better resiliency.
- Running more frequent simulations, rather than one or two a year, unsurprisingly drives up resiliency.
Evolution of phishing

• Fortune 50 organization

• The goal of a red team assessment is to ascertain whether or not a real world threat actor would be able to compromise the organization and gain access to specific trophy data.

• As part of this engagement, RSM added malicious capabilities to three USB devices (a drink warmer, a drink chiller, and a plasma ball) by rewiring the internal circuitry and including a malicious microcontroller.

• These three devices were each sent to individuals, **NOT SO RANDOMLY** chosen from the larger group.
  − Chosen from LinkedIn
Evolution of phishing

Webcam capture from compromised system
Security, Privacy and Risk in Healthcare

**CORE SERVICES**
- Penetration testing
- Policy and procedure review and development
- Firewall assessments
- Network architecture reviews
- Incident response tabletop

**SPECIFIC SERVICES FOR HEALTH CARE**
- Medical device risk management
- Ransomware readiness

**MAINTAIN CYBER RESILIENCE**
- Business process risk assessments
- Risk assessment and vulnerability management programs
- PCI report on compliance
- Social engineering
- Training

**ENHANCE VISIBILITY**
- Strategic and operational planning
- Virtual CISO
- Cybersecurity scorecard
- Risk analysis team
- Industry framework implementation

**EVOLVE CYBER STRATEGY**
- HIPAA risk analysis
- HIPAA compliance assessment
- Simulated OCR audit
- HITRUST readiness assessment
- HITRUST validated assessment

- HITRUST framework implementation
- Cyber due diligence for acquisitions
THANK YOU FOR YOUR TIME AND ATTENTION
Contact Info

**Anthony Catalano**
Director
216-927-8223
Anthony.Catalano@rsmus.com

**Greg Vetter**
Principal
217-372-1624
Greg.Vetter@rsmus.com