

# **Cybersecurity, HIPAA, Ransomware and New York's Cybersecurity Regulations**

**Speakers:**  
**Mitze Amoroso**  
**Noreen Gleason**  
**Tim Howard, Esq.**  
**Peter Resnick**  
**Francis J. Serbaroli, Esq.**



## HEALTH LAW

## Expert Analysis

# Cybersecurity in the Health Care Sector

As if it were not facing enough challenges, the health care industry is now becoming a more frequent target for hacking and ransomware by miscreants both domestic and foreign. Health care organizations have lagged behind other business sectors in protecting data, which is hard to understand given the extreme sensitivity of the data in their possession: personal and health information on individual patients; confidential information on internal quality assurance, risk management and utilization; results of clinical research on drugs, medical devices, and therapies; personal information on employees; sensitive internal financial information; confidential information on potential partnerships and deals with other organizations; and so on. Of even greater concern is the reality that hackers can interfere with web-connected medical equipment and devices and physically harm patients.

The Health Care Industry Cybersecurity Task Force, which was established by Congress in 2015, is comprised of representatives from both the government and private sector, and is charged with analyzing and making

By  
Francis J.  
Serbaroli



recommendations regarding securing and protecting the health care sector against cybersecurity incidents. S.754—114th Congress: Cybersecurity Information Sharing Act of 2015. The Task Force recently issued its “Report on Improving Cybersecurity in the Health Care Industry” (Report). The Report highlights the vulnerabilities to cyberattacks of organizations involved directly or indirectly in providing health care services and products, and makes recommendations to both the government and the industry to enhance awareness and improve protections.

### Industry

The Report begins by describing the industry as a “mosaic” of large health care systems, physician practices, public and private payors (e.g., Medicare, Medicaid, private insurers and plans), research institutions, medical device developers and manufacturers, software companies, as well as a large and diverse population of patients. It

observes that the continuing evolution of electronic health records and the health care industry’s extensive connectivity to the Internet have led to major improvements in both the quality and timeliness of patient care. The Report notes that the downside to these advances is that they have resulted in an increased attack surface for health care providers, medical device companies, and many other parts of the health care industry. The Report emphasizes that securing health care data as well as securing the operation of medical devices is essential to protecting patients and providing them with the highest level of medical care.

The Report makes recommendations to both the government and the industry to enhance awareness and improve protections.

Turning to the reality of cybersecurity and preparedness in the industry, the Report found that many health care organizations

lack the infrastructure to identify and track threats, the capacity to analyze and translate the threat data they receive into actionable information, and the capability to act on that information. Many

organizations also have not crossed the digital divide in not having the technology resources and expertise to address current and emerging cybersecurity threats. These organizations may not know that they have experienced an attack until long after it has occurred.

As to regulatory oversight, the Report finds that multiple federal agencies play a role in establishing and policing how health care organizations secure the privacy of their health care information, which has the potential to create complications:

Some entities may be subject to regulation and oversight by multiple federal government entities, each with their own rules, which may be difficult to reconcile. Product and technology innovations for medical devices and health IT outpace the development and creation of regulations.

Then there is the cost of compliance: While many regulations that apply to cybersecurity in health care are well-meaning and individually effective, taken together, they can impose a substantial legal and technical burden on health care organizations. These organizations must continually review and interpret multiple regulations, some of which are vague, redundant, or both. In addition, organizations must dedicate resources to implement policy directives that may not have a material impact on reducing risks.

### Recommendations

The Report includes six “high-level” imperatives, for each of which the Task Force provides a number of recommendations.

Imperative 1: “Define and streamline leadership, governance, and expectations for health care industry

cybersecurity.” To bring this about the Task Force recommends:

- creating a cybersecurity leader role within the U.S. Department of Health and Human Services (HHS) to align industry efforts for health care cybersecurity;
- establishing a consistent, consensus-based Cybersecurity Framework that is health-care specific, and includes standards, guidelines, and best practices;

---

The inherent vulnerabilities in the health care sector, together with the fact that health care will soon account for 20 percent of this country’s gross domestic product, make it all the more attractive to cyberattackers, and virtually guarantee that the problem will only get more serious and more complicated.

- requiring federal regulatory agencies to harmonize existing and future laws and regulations that affect health care cybersecurity;
- identifying scalable best practices for governance of cybersecurity across the health care sector; and
- exploring potential changes to the Stark Anti-Referral Law (42 U.S.C. §1395nn), the Anti-Kickback Statute (42 U.S.C. §1320a-7b(b)), and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners (e.g., physician practices).

Imperative 2: “Increase the security and resilience of medical devices and health information technology.” Specifically the Task Force recommends:

- securing legacy systems through compensating controls, device update, device retirement, network segmentation, etc.;
- improving manufacturing and development transparency among software developers and users;
- increasing the adoption and rigor of the secure development lifecycle (from concept generation through end of life recycling or disposal) in the development of medical devices and electronic health records;
- requiring strong authentication to improve identity and access management for health care workers, patients, medical devices and electronic health records;
- employing strategic and architectural approaches to reduce the attack surface for medical devices, electronic health records, and their interfaces; and
- establishing a Medical Computer Emergency Readiness Team to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures.

Imperative 3: “Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.” To that end, the Task Force recommends:

- requiring every health care organization to identify the cybersecurity leadership role (e.g., chief information security officer) for driving more robust cybersecurity policies, processes and functions, with involvement of senior executives;
- establishing a model for adequately resourcing the cybersecurity workforce with qualified individuals, and determining an acceptable ratio of health care cybersecurity expertise to the size

of the organization, complexity of care, degree of interconnectedness with other organizations, etc.;

- creating managed security service providers (MSSP) models to support small and medium-sized health care providers so they can have state-of-the-art security monitoring, defensive and reporting capabilities; and
- evaluating options for small and medium-sized health care providers to migrate patient records and legacy systems to secure environments such as hosted, cloud, and shared computer environments.

Imperative 4: “Increase health care industry readiness through improved cybersecurity awareness and education.” The Task Force believes this can be accomplished by:

- developing education programs targeting executives and boards of directors about the importance of cybersecurity education;
- ensuring existing and new products/systems’ risks are managed in a secure and sustainable fashion through “cybersecurity hygiene” (i.e., an evaluation of each individual’s security practices and precautions when conducting activities online);
- establishing an assessment model for evaluating a health care organization’s conformity with cybersecurity hygiene that regulatory agencies and industry can rely upon;
- customizing the Baldrige Cybersecurity Excellence Builder, a cybersecurity self-assessment tool created by the National Institute of Standards and Technology, for use by health care organizations;
- increasing outreach and engagement for cybersecurity across all levels of government and the private

sector through a cybersecurity education campaign involving both HHS and the Department of Homeland Security; and

- providing patients with information on how to manage their health care data to enable them to make educated decisions when selecting services or products from non-regulated entities (e.g., fitness trackers, devices and other consumer health care/lifestyle products).

Imperative 5: “Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.” The Task Force recommends:

- developing guidance for industry and academia on creating economic impact analysis and loss for cybersecurity risk for health care research and development; and
- pursuing research into protecting health care “big data” sets.

Imperative 6: “Improve information-sharing about industry threats, risks, and mitigations.” The Task Force outlined the following steps to accomplish this:

- make information-sharing on threats and risks easier among small and medium-size health care organizations that rely on limited or part-time cybersecurity staff;
- create more effective mechanisms for disseminating and utilizing data about threats, vulnerabilities and incidents; and
- encourage cybersecurity annual readiness exercises by the health care industry to prevent uncoordinated and ineffective responses to cyberattacks.


## Conclusion

The Task Force’s Report is a wake-up call to every organization in the health

care sector, large or small. Cyberattacks are increasing and becoming even more dangerous. The inherent vulnerabilities in the health care sector, together with the fact that health care will soon account for 20 percent of this country’s gross domestic product, make it all the more attractive to cyberattackers, and virtually guarantee that the problem will only get more serious and more complicated.

Health care organizations that do not recognize these dangers or take effective steps to mitigate them are not only doing a disservice to their patients or customers, they are risking their reputations and subjecting themselves to costly notification processes and remediation expenses, as well as regulatory crackdowns, class action lawsuits, significant penalties and legal liabilities, and the potential separation from employment of the senior executives on whose watch the problem occurred. Placed in that context, expenditures on appropriate cybersecurity protections look like a wise investment.





Hot Topics in Cyber Risk  
Facing the Ransomware Menace:  
Cyber Blackmail

January 24, 2018  
New York, NY

CRA Charles River Associates

---

---

---

---

---

---

---

---

---

---

### 6 things to include in your incident response plan

When corporate data are moved to the cloud, key access logs and other forensic artifacts can get moved as well. Follow the tips below before an incident occurs to ensure that your incident response team can preserve access to these critical data stores.

<p><b>ACTIVATE ACCESS LOGS AND TRACKING</b></p> <p>Ask your cloud provider to activate access logs and other tracking mechanisms. Confirm that the logs are being retained for the time period that matters to you.</p>	<p><b>VALIDATE SCALABILITY</b></p> <p>You may have a plan in place to search a single mailbox or a single day's worth of activity. However, can you quickly and effectively search for evidence of intrusion across all employees over a multiple-month time frame?</p>
<p><b>NEGOTIATE A RESPONSE AGREEMENT</b></p> <p>Memorialize a service level agreement with your cloud provider that includes breach incident response. This should include a process, a price, and an agreed-upon response time.</p>	<p><b>CONFIRM EVERYTHING</b></p> <p>Does your cloud provider have the desired security? Insurance coverage? Cyber disaster recovery protocols in place? Confirm all of these things periodically.</p>
<p><b>HOLD "CYBER FIRE DRILLS"</b></p> <p>Periodically test your incident response plan to ensure that it continues to function as expected and as needed.</p>	<p><b>FIND AN INDEPENDENT EXPERT</b></p> <p>Retain an experienced incident response team via outside counsel to reasonably establish and preserve attorney-client privilege. This is vital since it is likely that the findings and conclusions will be of significant interest to third parties who will have interests adverse to your own.</p>

CRA Charles River Associates

---

---

---

---

---

---

---

---

---

---

### What will you do when your company is asked to pay a ransom?

What conversations need to occur now – at your company and with your board – and how will you weight the relevant legal, ethical, practical, and public policy considerations?



CRA Charles River Associates

---

---

---

---

---

---

---

---

---

---

### Reduce the risk and cost of a data breach

A well thought out strategy can dramatically reduce the likelihood and severity of a data incident. Follow the tips below to help reduce your risks.

- 01 Engage the board**  
This critical step will improve risk oversight and help demonstrate fiduciary obligations were fulfilled.
- 02 Strengthen your defenses**  
Up-to-date policies and procedures will help prevent/detect/contain potential breaches.
- 03 Consolidate your data**  
Reduce the amount of data that you maintain and the number of tools and personnel who can access it.
- 04 Understand your attackers**  
Will their motivation be ransom-as-a-service? Trade secrets and other confidential information? Sabotage?
- 05 Limit data access**  
Keep your customer data on secure, encrypted company networks that are accessible only by authenticated users.
- 06 Purchase insurance**  
Contingent business interruption insurance covers your losses when your cloud provider experiences an interruption to its business operations.

4 Private and Confidential




---

---

---

---

---

---

---

---

---

---

### Be prepared for class action litigation

Companies that experience a data breach face a very real risk of class action litigation. Make sure your company understands the parties who may be involved, and potential causes of action.



5 Private and Confidential




---

---

---

---

---

---

---

---

---

---

### What cyber damages can you recover?

Because cyber damages can be challenging to quantify, companies risk making business, legal, and disclosure decisions based on incomplete estimates of the comprehensive economic impact of a cyber incident.



6 Private and Confidential




---

---

---

---

---

---

---

---

---

---



### Maximize your cyber insurance coverage

Will your company's insurance adequately mitigate the economic impact of a cyber incident? The time to perform a coverage assessment is now – and periodically thereafter.

#### Cyber policies

Cyber policies typically cover a range of expenses incurred in a data breach, including:

- Notification costs
- Penalties
- Credit monitoring
- Costs to defend regulatory claims
- Fines
- Business Interruption

#### Non-cyber policies

You don't necessarily need a policy with the word "cyber" in it. If your company has one of the policies below, you may already have some level of coverage in the event of a cyber incident.

 <p><b>Kidnap and ransom insurance</b> Some policies cover situations where computers and systems have been "constructively kidnapped" by ransomware.</p>	 <p><b>Directors and officers (D&amp;O) policy</b> Covers legal expenses if named as defendants in a cyber-related shareholder action.</p>
 <p><b>Property insurance</b> Policies written on an "all-risk" basis may cover physical damage caused by malware.</p>	 <p><b>Professional liability/errors and omissions policies</b> Some policies can cover losses resulting from when an employee makes a mistake resulting in cyber-related damage (e.g., spread of malware).</p>
 <p><b>Fidelity (or "crime") insurance</b> May cover situations of employee-caused theft or sabotage.</p>	 <p><b>General liability</b> Some policies may indemnify and provide a defense against a wide variety of claims, including claims alleging invasion of privacy rights and some policies may afford coverage for theft of consumer data, misuse of customer information, copyright infringement, and other types of unfair competition.</p>

7 Private and Confidential



---

---

---

---

---

---

---

---

---

---

### Regulatory expectations after a data breach

The U.S. Securities and Exchange Commission has outlined the following guidance for registrants who experience a ransomware and/or cybercrime incident:



8 Private and Confidential



---

---

---

---

---

---

---

---

---

---

**To continue the conversation**  
 Peter Resnick, CPA/CFF, CFE  
 Vice President, Forensic Services  
 at +1-617-425-6587 or presnick@crai.com

Kristofer Swanson, CPA/CFF, CFE, CAMS  
 Vice President and Practice Leader, Forensic Services  
 at +1-312-619-3313 or kswanson@crai.com

9 Private and Confidential



---

---

---

---

---

---

---

---

---

---







## Cyber Security

# What keeps a CIO up at night...

**Presented by: Mitze Amoroso**  
Senior Vice President/Chief Information Officer

Together, We Can...January 24, 2018

---

---

---


---

---

---

---

---



**INFORMATION TECHNOLOGY**

## Security Vision

Ensure the confidentiality, integrity and the availability of information, assets and resources

Together, We Can...

---

---

---

---

---

---

---

---



**INFORMATION TECHNOLOGY**

## Threats in Healthcare

**Ransomware** Ransomware is a type of malicious software or from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. [Wikipedia](#)

**Phishing** Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. [Wikipedia](#)

**Medical Devices** Tele-medicine devices

**Worms/Malware** Computer worm is a type of malicious software program (malware) that, unlike viruses, replicates itself by modifying other computer programs and inserting itself into them. [Wikipedia](#)

**Third Party** Consultants, vendors who have access to your data

**Users** Employees, users

Together, We Can...

---

---

---

---

---

---

---

---

INFORMATION TECHNOLOGY 

### The Solution



### Multi-Layered Security Approach

Together, We Can...

---

---

---

---

---

---


---

---

### MULTI-LAYERED APPROACH

Firewall

FIREWALL



---

---

---

---

---

---


---

---

### MULTI-LAYERED APPROACH

Web/Spam Filters

Web/Spam Filters



---

---

---

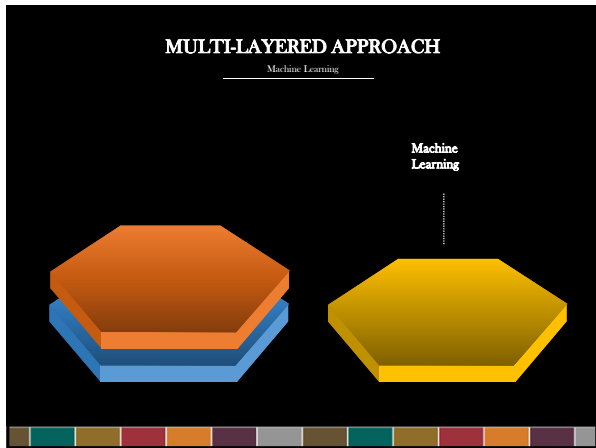
---

---

---

---

---



---

---

---

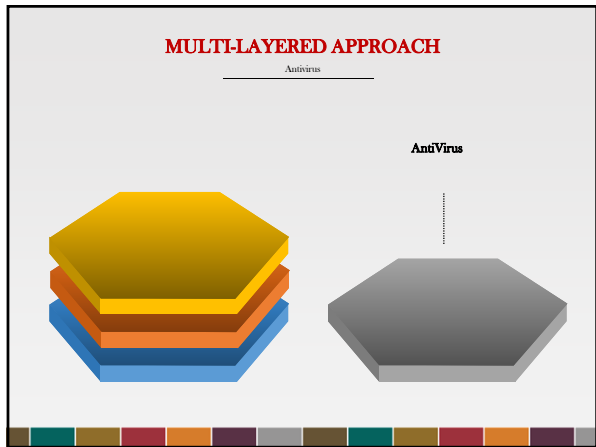
---

---

---

---

---



---

---

---

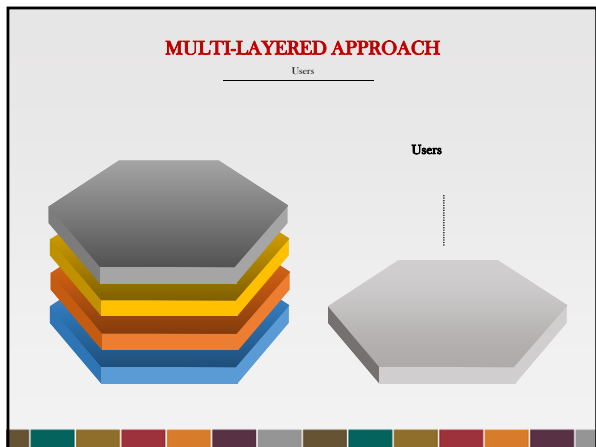
---

---

---

---

---



---

---

---

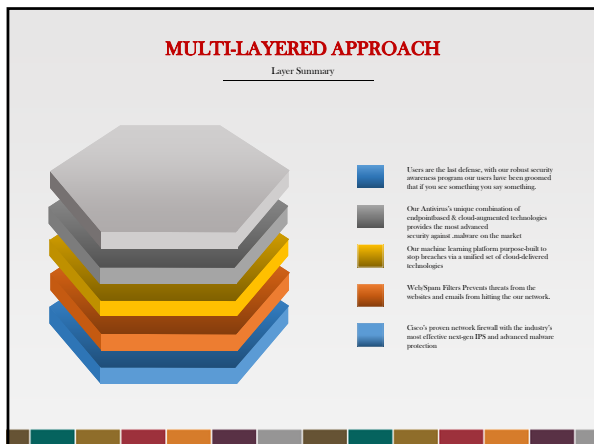
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

---

---

**INFORMATION TECHNOLOGY**

## How to Mitigate the Threats

- **Patch, Password and Backup Management**  
Patching all equipment timely, strong Password and successful backups
- **Vulnerability and Threat Assessment**  
Scan for vulnerabilities everywhere, accurately and efficiently. You need to examine the network vulnerabilities over time at different levels of detail. Not just single snapshots
- **Plans / Reports**  
At a minimum you need to have a Disaster Recovery, Business Continuity, Incident Response Plan and a Risk Assessment done.
- **Security Awareness Programs**
  - Monthly Security Videos
  - Tech Tip Tuesday's, Screen Savers
  - Phishing Campaigns
  - Dark Web

**Together, We Can...**

---

---

---

---

---

---

---

---

---

---

---

---

**INFORMATION TECHNOLOGY**

## Samples of Collected Security Statistics

#### Vulnerabilities

#### EMAILS

EMAIL Statistics [inbound]	TOTAL	DATE	WEEK
Blocked	5,689,687	4,266	672
Blocked Virus	223,042	1	0
Rate Controlled	2,308,652	242	8
Quarantined	16,424	26	4
Allowed Tagged	9,376	4	0
Allowed	5,287,287	4,028	639
<b>Total Received</b>	<b>17,637,487</b>	<b>8,567</b>	<b>1,215</b>

In December, **AntiVirus** Blocked 146 Threats

In the last 30 days, **Machine Learning System** Blocked 41 Threats, 0 Critical, 0 High

**Together, We Can...**

---

---

---

---

---

---

---


---

---


---

---

---


 archcare  
The Continuing Care Community  
of the Archdiocese of New York

# Thank you



Mitze Amoroso  
Senior Vice President, Chief Information Officer  
Office: 646-505-3860  
Email: mamoroso@archcare.org

**Together, We Can...**



---

---

---

---

---

---

---

---