Security and the C-Suite
Leadership’s Role in Building a Cyber-Resilient Organization
Allyson Vicars
Consultant, Research
vicarsa@advisory.com
February 15, 2018
2018 National Meeting

Beyond Meaningful Use and Operational Excellence

2018 Session Dates and Locations

- **Chicago, IL**
  - July 25-26
- **Marina del Rey, CA**
  - June 27-28
- **Dallas, TX**
  - June 13-14
- **Washington, DC**
  - May 16-17
  - August 14-15

2018 National Meeting Agenda

- State of the Union
- IT’s Role in the New Cost Control Mandate
- Digital Health Systems
- Quality Reporting Office Hours
- The Decision Machine - Analytics and the Rise of AI
- The Era of the Connected Patient

*Catch the highlights from our 2017 series on-demand.*

Registration Now Open
Register [here](#)
Security and the C-Suite

Leadership’s Role in Building a Cyber-Resilient Organization
All Executives Must Be Engaged in Security

“
The time has come for CEOs and Boards to take personal responsibility for improving their companies’ cyber security. Global payment systems, private customer data, critical control systems, and core intellectual property are all at risk today. As cyber criminals step up their game, government regulators get more involved, litigators and courts wade in deeper, and the public learns more about cyber risks, corporate leaders will have to step up accordingly.”

Sameer Bhalotra
Former White House Senior Director for Cybersecurity
1. Current State of Security Affairs

2. Senior Leadership That Drives Cyber-Resiliency

3. The Long Game: A Path Toward an Adaptive Security Posture
Health Care Is Increasingly a Target

Escalating Financial Stakes for Breaches

Percent of Breaches by Industry¹

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>24%</td>
</tr>
<tr>
<td>Health Care</td>
<td>15%</td>
</tr>
<tr>
<td>Retail and Accommodation</td>
<td>15%</td>
</tr>
<tr>
<td>Public</td>
<td>12%</td>
</tr>
</tbody>
</table>

Selection of 2017 OCR³ Fines and Settlements

- **Anthem**: $115M
- **Memorial Healthcare System**: $5.5M
- **Memorial Hermann Health System**: $2.4M

63% Percent increase in major cyberattacks against health care organizations in 2016²

---

² Sheridan K, "[Major cyberattacks on healthcare grew 63% in 2016](https://www.darkreading.com)," Dark Reading, December 2016.
³ OCR = Office for Civil Rights.
Increasingly Sophisticated, Quickly-Evolving Threats

Powerful Nation-State Exploits Now Available to Anyone Online

Timeline of Recent Release and Use of Nation-State Exploits

<table>
<thead>
<tr>
<th>August 2016</th>
<th>May 12, 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shadow Brokers steal a cache of exploits from Equation, a group allegedly tied to NSA</td>
<td>EternalBlue exploit used for WannaCry attack that encrypted files for ransom</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>April 14, 2017</th>
<th>June 27, 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shadow Brokers post and auction off 15 NSA exploits with goal of raising 1M bitcoin</td>
<td>NotPetya wiped files with no intention to restore; collateral damage from cyberwarfare</td>
</tr>
</tbody>
</table>

WannaCry a Sloppy Campaign—Don’t Expect a Simple Solution Next Time

*Cyber Criminals Willing to Cause Significant Damage for Modest Profit*

- **$4B–$8B**
  - Estimated worldwide total economic damage

- **$55K**
  - Profit made by “amateurish” attackers

- **$10.96**
  - Cost to register domain that stopped the attack

1) NSA = National Security Agency.

Source: Health Care IT Advisor research and analysis.
Early Stages of Coordinated Industry Response

National-, Industry-, and Community-Level Information Sharing Underway

Infragard
(National, Across Multiple Industries)
Partnership between FBI¹ and private sector to collaborate to protect Critical Infrastructure

National Health Information Sharing and Analysis Center
(National, Health Care Specific)
Non-profit dedicated to sharing cyber and physical security threat indicators and defense strategies with its members

Medical Device Vulnerability Intelligence Program for Evaluation and Response (MD-VIPER) (Medical Device Specific)
Partnership between NH-ISAC, MDISS,² and the FDA³ through which members can learn and mature efficient value-added risk assessment, vulnerability information sharing, and surveillance components

Case in Brief: Intermountain Joint Cybersecurity Operations Center

- Created joint 24/7 security operations center about two years ago
- Joint venture amongst six different organizations, including Intermountain Healthcare
- Goal to share a “playbook” of resources on information security
- An advance beyond protecting the perimeter to anticipating the next attack

---

¹ FBI = Federal Bureau of Investigation.
² MDISS = Medical Device Innovation, Safety, and Security Consortium.
³ FDA = Food and Drug Administration.

Sources: Infragard; NH-ISAC; MD-VIPER; Health Care IT Advisor research and analysis.
# Technology Basics Present or Moving into Place

## Surveys Show Investment in Security Technologies Growing

### 2017 Health Care IT Advisor Cybersecurity Survey Results

**Percentage of Survey Respondents Who Use the Following Technical Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block personal email on network</td>
<td>34%</td>
</tr>
<tr>
<td>Use cyber intelligence</td>
<td>56%</td>
</tr>
<tr>
<td>Use multi-factor authentication</td>
<td>65%</td>
</tr>
<tr>
<td>Use single sign-on</td>
<td>74%</td>
</tr>
<tr>
<td>Use intrusion detection and response systems</td>
<td>84%</td>
</tr>
<tr>
<td>Conduct penetration tests at least annually</td>
<td>85%</td>
</tr>
</tbody>
</table>

### 2017 HIMSS Cybersecurity Survey

**Percentage of Organizational Budget Allocated to Cybersecurity**

<table>
<thead>
<tr>
<th>Percentage of Budget Allocated</th>
<th>Percentage of Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>11% More than 10% of budget</td>
<td>11%</td>
</tr>
<tr>
<td>17% 7%-10% of budget</td>
<td>17%</td>
</tr>
<tr>
<td>32% 3%-6% of budget</td>
<td>32%</td>
</tr>
<tr>
<td>40% 1%-2% of budget</td>
<td>40%</td>
</tr>
</tbody>
</table>

1) Chart represents only organizations that indicated they allocate “some amount” to cybersecurity (71%), 21% did not know, and 8% dedicate “no specific amount.”

Sources: 2017 Health Care IT Advisor Cybersecurity Survey results, November 2017; 2017 HIMSS Cybersecurity Survey; Health Care IT Advisor research and analysis.
Efforts to Address the Human Element Lag

C-Suite Push Back Potentially Stunting Frequent Awareness Testing

Frequency of Security Awareness Training

- Continually: 53%
- Annually: 37%
- Quarterly: 5%


Frequency of Internal Phishing Campaigns

- Continually: 27%
- Monthly: 15%
- Yearly: 39%
- A few times a year: 8%
- Never: 11%

Key Lesson: The more frequent the testing, the better the results.
Aware, Concerned…and Delegating Responsibility

Formal Delegation of Responsibility Doesn’t Absolve Accountability

**Improved Awareness in C-Suite and Board**

Moving beyond the check-the-box mentality, but deep understanding lags

67% of survey respondents discuss cybersecurity regularly with their board

---

**...But Who Should Be Responsible?**

35% of C-level executives said IT teams would be responsible for a breach, while 50% of IT leaders say responsibility lies with senior managers

---

**Action Often Left for the CIO to Lead**

66% of health care CISOs report to their CIOs

Technical controls will fall on the IT organizations regardless

---

1) [2017 HCITA Cybersecurity Survey](#), November 2017.
3) [Operationalizing Cybersecurity in Healthcare Organizations](#), Symantec and HIMSS Analytics, 2017.

Source: Health Care IT Advisor research and analysis.
## Harness the Positive Momentum to Activate Leaders

### Defining Roles for Senior Leaders Quells Complacency

Where would each of your leaders fall on this spectrum?

<table>
<thead>
<tr>
<th>Disengagement or Passive Support</th>
<th>Activated Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Cyber-what?”</td>
<td>“I am knowledgeable of industry threats and proactively ask questions.”</td>
</tr>
<tr>
<td>“That’s why we have a CISO… it’s someone else’s problem.”</td>
<td>“This is an enterprise risk for which I am personally accountable.”</td>
</tr>
<tr>
<td>“Tell me just enough for due diligence because I’m uncertain of my role in this.”</td>
<td>“I am accountable, therefore I have a role to play as a leader.”</td>
</tr>
<tr>
<td>“Why bother? There’s nothing we can do about it.”</td>
<td>“I enable and promote cyber resiliency within our organization.”</td>
</tr>
</tbody>
</table>

Some individuals may **lead** while others **lag** in engagement.

Source: Health Care IT Advisor research and analysis.
Providers Are an Attractive Target for Cyber Criminals

Understand Why HCOs Are Targeted to Identify Areas for Improvement

Complex IT Systems with Marketable Data
- Multiple databases and interactions between vendors, partners, and affiliates
- Hundreds of medical devices
- Valuable data for sale including protected health information (PHI), financial, and clinical data

Lack of Robust Security Controls
- Lack of data encryption
- Fragmented identity management and access control
- Under investment in monitoring resources
- Weak disaster recovery and business continuity
- Lack of threat intelligence

Under-Engaged, Under-Involved Leadership
- Senior leaders often not knowledgeable about threats or about their roles in reducing risk
- Poor incident response preparedness
- No clear understanding of who makes decisions during an incident

Reactive vs. Proactive Culture
- Culture of openness and helpfulness; staff motivated to help others; often naïve about potential threats
- High-pressure work environments can result in low tolerance for preventative measures that lower risk at the expense of slowing operations

Source: Health Care IT Advisor research and analysis.
The Cybersecurity Ecosystem Model

Leadership Role Extends Beyond the Purchase of Technical Tools

Governance and Policy
- C-Suite and Board Engagement
- Dashboards
- Governance Standards
- Strategy
- Digital Trading Partners
- Staffing

Cyber Resilient Organizations

Process and Education
- Training
- Testing
- Incident Response Planning
- Audits
- Business Continuity Planning + Back-ups + Disaster Recovery
- Risk Assessments

Technology and Services
- Cyber Intelligence
- IT-Enabled Capabilities
- Cyber Insurance
- Information Sharing

Source: Health Care IT Advisor research and analysis.
1 Current State of Security Affairs

2 Senior Leadership That Drives Cyber-Resiliency
   - Tips for cybersecurity conversations
   - Messages for IT leaders to deliver to the C-suite
   - Tactics to activate and involve C-suite in cyber efforts

3 The Long Game: A Path Toward an Adaptive Security Posture
Relevant Opportunity Areas for Senior Leadership

Governance and Policy
- C-Suite and Board Engagement
- Dashboards
- Governance Standards
- Strategy
- Digital Trading Partners
- Staffing

Process and Education
- Training
- Testing
- Incident Response Planning
- Audits
- Business Continuity Planning + Back-ups + Disaster Recovery
- Risk Assessments

Technology and Services
- Cyber Intelligence
- IT-Enabled Capabilities
- Cyber Insurance
- Information Sharing

Source: Health Care IT Advisor research and analysis.
Marshal Your Executive Allies

Build a Foundation with Private Meetings

Awareness and Interest in Cyber Risk Growing Amongst Senior Leadership

*Attitudes Vary But Can Be Under- or Misinformed*

Hold One-on-One Closed-Door Meetings with Key Executives

*Explore on an Individual Basis:*

- **General attitude about risk and security**
- **Level of cybersecurity knowledge**
- **Underlying concerns around risk and security**

You are there to **listen**, not educate.

Source: Health Care IT Advisor research and analysis.
A Framework for a Successful Security Discussion

Goal Is to Inspire Dialogue and Engage Senior Leadership

Prepare in Advance

- Make sure you understand the organization’s current state
- Hold private meetings with key leaders to understand their concerns and perspectives

Prepare in Advance

Keep It Simple

- Talk in business terms and leverage scenarios to illustrate the organization’s risk profile from various threats
- Discuss improvements made to lower risk

Be Clear About Alternatives

- Provide alternatives for changing the organization’s risk posture
- Acknowledge trade-offs for each alternative

Discuss Roles

- Provide examples of various roles they can play in managing cyber risk
- Ask for their guidance and assistance

Listen and be flexible to the flow of the conversation

Source: Health Care IT Advisor research and analysis.
Cybersecurity Touches All Enterprise Risk Domains

Potential Reality: “Please Only Contact Us in a Genuine Emergency”

Actual tweet from a provider organization affected by WannaCry

<table>
<thead>
<tr>
<th>Domain</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>Cannot see patients due to a major ransomware attack</td>
</tr>
<tr>
<td>Strategic</td>
<td>M&amp;A deal falls through due to a publicized breach</td>
</tr>
<tr>
<td>Human Capital</td>
<td>Terminate staff due to inappropriate chart access</td>
</tr>
<tr>
<td>Technology</td>
<td>A year’s worth of data lost or otherwise inaccessible</td>
</tr>
<tr>
<td>Clinical/Patient Safety</td>
<td>No access to patient record during unexpected outage</td>
</tr>
<tr>
<td>Financial</td>
<td>OCR levies fines due to poor security and privacy controls</td>
</tr>
<tr>
<td>Legal/Regulatory</td>
<td>Face class action lawsuits from affected individuals</td>
</tr>
<tr>
<td>Hazard</td>
<td>Are you still secure when a natural disaster strikes?</td>
</tr>
</tbody>
</table>

Erie County Medical Center spent nearly $10M recovering from massive cyberattack

The Buffalo News, July 26, 2017

“Richard Harvey, 50, was about to undergo surgery… following a motorcycle accident when a nurse told him [it] had been cancelled because of a cyberattack”

Washington Post, May 12, 2017

“Please be aware that [we] are experiencing serious IT problems … please only contact [us] in a genuine emergency”

Actual Tweet from an NHS Trust during WannaCry

1) M&A = Mergers and acquisitions.
2) NHS = National Health Service (provider organization).

Source: Health Care IT Advisor research and analysis.
There Is a Personal and Public Liability

Consequences Rise to the Board and C-Suite Level

**Chief Executive Officer**
Dido Harding, CEO of TalkTalk, forced to resign in 2017 in fallout from a 2015 customer data breach

**Chief Legal Counsel**
Ron Bell, Chief Legal Counsel for Yahoo! fired following a second major breach, reportedly taking the fall for the CEO

**Board Members**
All board members of Helse Sør-Øst, largest Norwegian health authority, fired after 2.8M records breached

**Chief Financial Officer**
CFO of FACC aerospace firm fired after a whaling attempt convinced him to transfer 50M€ to criminals; CEO fired a few days later

---

**Case in Brief: Banner Health**
- Large non-profit health system with 28 hospitals based in Phoenix, AZ
- Cyber attackers hacked payment card from food, beverage outlets and a patient data system
  - Affected 3.7M people including patients, providers, plan members, and beneficiaries
- Facing class-action lawsuit which claims the organization failed to maintain adequate security measures and sues for more robust remediation (led by one of their physicians)

Source: Health Care IT Advisor research and analysis.
Pertinent Board Member Backgrounds Are Critical

Valuable Experience from In and Outside Health Care, Technology

Leverage a Variety of Backgrounds to Enhance Security Oversight

CISO, Global Shipping Firm
- Brings technical expertise
- Functions as an advisor
- Challenges recommendations to improve them

CIO, State University
- Helps with planning, investment, strategy
- Understands interconnectivity of security and IT
- Prioritizes security

CEO, Banking Industry
- Understands regulatory demands
- Brings external industry expertise

Resource: World Economic Forum Principles for Boards on Cyber Resilience
- Board should perform a self review of its own performance on cybersecurity
- Board should periodically review its own composition to ensure it adequately oversees cybersecurity
  - Do board member backgrounds include sufficient experience and skills to promote cyber resilience?
  - Would the addition of a cyber resilience expert help the board meet their fiduciary responsibility?

Ten Board Principles for Cyber Resilience

Responsibility for cyber resilience
Board takes ultimate responsibility for oversight of cyber risk and resilience with ability to delegate primary oversight to a committee

Accountable officer
Board ensures that one corporate officer is accountable for reporting on the organization’s cyber resilience capabilities and goal implementation progress

Risk assessment and reporting
Board holds management accountable for consistent reporting of a quantified and understandable assessment of cyber risks and threats and validates these assessments using its Cyber Risk Framework

Integration of cyber resilience
Board ensures the incorporation of cyber resilience and risk management into the enterprise’s overall business strategy

Resilience plans
Board ensures management creation, implementation, testing and ongoing improvement of cyber resilience plans and requires the accountable officer to monitor performance and regularly report to the board

Command of the subject
Board members receive an orientation to cyber resilience upon joining and are regularly updated on threats and trends

Risk appetite
Board annually defines and quantifies business risk strategy relative to cyber resilience and ensures its consistency with enterprise risk management

Community
Board encourages management collaboration with other relevant stakeholders to ensure system-wide cyber resilience

Effectiveness
Board periodically evaluates its own performance in implementing these principles or seeks independent advice

Seize Every Opportunity to Educate

Orientation Allows for Individualized Training Tuned to Board-Level Role

Kaiser Permanente’s Board Education Efforts

New Board Member Security Orientation
- Update on current external threats
- Review of existing technological defenses and current strategy
- Review of internal people campaigns
- Walkthrough of risk dashboards

Key Questions
1. Does your organization conduct any new board member orientation?
2. Is sufficient cybersecurity training included as part of that orientation?
3. Do you know who organizes it and can you get in contact with him or her?
4. Do you have material to use that is at the right technical level?
5. Does your material illustrate how the organization governs, not manages, security?
6. How will you manage updates to the material to reflect the organization’s ever-evolving security posture?

Continuing Education with Frequent Updates
- Update board quarterly
- Provide *ad hoc* training upon request during regular teaching segments
- Review risk dashboards

Sources: Kaiser Permanente; Health Care IT Advisor research and analysis.
Facilitate Informed and Standardized Decisions

Build in Automatic Consideration for Tradeoffs

**UVA Health System Process for Executive Management Security Decisions**

*Decision framework applies to all security-related technology, policy, or process decisions*

**Annual Assessment Program**
- Rolling internal assessments to determine overall status
- External consultant assesses technology, policies, adherence, and provides a gap analysis
- Separate third-party penetration test

**Security Recommendations**
- CIO and CISO use assessment results to pinpoint high-priority areas
- Develop set of security recommendations for the year to request from the institution

**Standardized Security Decision Framework**
- **Cost**
- **Disruption**
- **Inconvenience**

Thorough assessments from internal and external vendors identify areas for biggest “bang for your buck”

Illustrate **continuity** of recommendations from year to year.

Sources: UVA Health System; Health Care IT Advisor research and analysis.
Direct Their Focus to What They Care About

Metrics Used to Manage the Security Team Often Distract Leadership

What Can Senior Leaders Do with These Operational Metrics?

87K

- Number of attacks last month

25%

- Percentage of unpatched vulnerabilities

45 minutes

- Median time-to-remediation

68K

- Number of malicious emails blocked

“Raw metrics are valuable from an operations standpoint, but at the executive level, it’s about a **cohesive story**.”

Adam Ely, CSO and Founder
Bluebox Security

---

Consider Tracking to a Security Standard

Metro Health’s Tiered Approach Focuses Board on High-Level Progress

Depiction of Board-Level Dashboard

<table>
<thead>
<tr>
<th>Category</th>
<th>Project #1</th>
<th>Project #2</th>
<th>Project #3</th>
<th>Project #4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example Operational Metrics

- **50%** Increase in malicious emails
- **20%** Increase in “clickers” in phishing campaigns
- **45 hours** Spent on critical vulnerability patching

High Level
- Tracks performance against NIST

Ongoing Improvement Efforts
- Projects in progress to improve performance in NIST categories

Department Level
- Granular metrics available, if needed, to explain progress

Sources: Metro Health (Grand Rapids, MI); Health Care IT Advisor research and analysis.
Find a Dashboard That Fits Your Board

Consider Tracking Maturity Instead of Risk

<table>
<thead>
<tr>
<th>Org. Priority</th>
<th>Security Control Group</th>
<th>Description</th>
<th>LY Maturity Level</th>
<th>Current Quarter Maturity Level</th>
<th>YE Maturity Level</th>
<th>YE+1 Maturity Level</th>
<th>Action(s) in CY Top 10 Initiatives?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Systems &amp; Security Management</td>
<td>Hardware and software authorization, tracking, management, secure configuration, and security protections</td>
<td>Low</td>
<td>Developing-Developing</td>
<td>Developing-Moderate</td>
<td>Moderate</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Vulnerability Management</td>
<td>Ongoing systems vulnerability management through testing and remediation and conducting in depth security and penetration testing.</td>
<td>Developing</td>
<td>Developing-Moderate</td>
<td>Moderate-High</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Network Perimeter (Internet) Security</td>
<td>Ensuring appropriate security controls, configuration, and oversight in place for networks and technology which provide pathways to/from the Internet (such as firewalls, proxy services, e-mail, etc)</td>
<td>Developing</td>
<td>Moderate</td>
<td>Moderate-High</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Data Protection</td>
<td>Identification, classification, encryption and data loss prevention of confidential information.</td>
<td>Low</td>
<td>Developing</td>
<td>Moderate-High</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Data Recovery/ Business Continuity</td>
<td>Ability of organization to recover from a localize or larger scale IT service or data interruption event.</td>
<td>Developing</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate-High</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Security Incident Response</td>
<td>Incident response protocols, process, technologies and skillsets to enable an effective response to threats or incidents.</td>
<td>Moderate</td>
<td>Moderate-High</td>
<td>High</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>User Access Management</td>
<td>User and administrative account management, security monitoring and access permissions auditing and oversight.</td>
<td>Moderate</td>
<td>Moderate-High</td>
<td>High</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>Privacy and Security Monitoring</td>
<td>Maintenance, monitoring and analysis of security and privacy related audit logs</td>
<td>Developing</td>
<td>Moderate</td>
<td>Moderate-High</td>
<td>Moderate-High</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Network Security Management</td>
<td>Secure configuration and oversight of networking equipment, including firewalls and wireless networks.</td>
<td>Developing</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate-High</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>Securely Managed Applications</td>
<td>Applications developed and implemented in a secure manner</td>
<td>Developing</td>
<td>Developing</td>
<td>Developing</td>
<td>Developing</td>
<td>No</td>
</tr>
</tbody>
</table>

Source: MaineHealth, sample data.
Intuitive, Actionable Board-Level Dashboard Options

Target-Level Maturity Requires Discussion, Negotiation, and Tradeoffs

<table>
<thead>
<tr>
<th>Capability Area/Domain¹</th>
<th>Rudimentary</th>
<th>Foundational</th>
<th>Baseline</th>
<th>Advanced</th>
<th>Cutting-Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Strategy and Operating Model</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Risk Reporting and Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Infrastructure Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Application Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vigilant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Threat Intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resilient</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Incident Readiness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Incident Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹) Number of domains illustrated has been truncated to fit the slide.

Caution: Too Many Factors Can Cloud Effectiveness

Classic Spider Diagram Useful for Tracking Status of Several Categories

C-Suite Involvement Promotes Voice from Outside IT and Security

Five Key Security Governance Activities

**Structure**
- Get organized:
  - Committee structure
  - Whom to involve
  - Roles (champion, creator, owner, user, auditor, etc.)

**Monitor**
- Ensure risk assessments, audits, penetration tests are done, results tracked, and remediation completed

**Identity and Access Governance**
- Establish role-based access and provide exception processes

**Strategy**
- Ensure there is an appropriate security strategy in place and monitor progress of implementation (roadmap)

**Key Policies**
- Ensure adherence to key policies, calibrating them to fit culture of the organization and meet workflow needs of users

Source: Health Care IT Advisor research and analysis.
Incorporate Feedback from Across the Organization

Consultative Model Builds Trust and Buy In, Allows for Negotiation

Security Governance at Texas Health Resources

Multidisciplinary Information Services Security Governance Council

**Executive Representation**

- Chief Compliance Officer*
- CIO*
- Finance
- Human Resources
- Privacy
- Supply Chain
- Clinical Engineering
- Legal
- At least 2 physicians

*Co-Chairs

**Operational Governance Review**

- System-Level Decisions

**Frameworks**

- Final Review

**Single Disciplinary Committees**

- Physician Leadership
- Nursing Leadership
- Operations Leadership

**Information Security**

- Architects all security recommendations (policies, processes, and investment decisions) within the framework
- Provides quarterly security updates to the council
- Ensures council agrees with direction of security program

IT/Security requests insight and opinion before drafting recommendation

IT/Security requests approval or disapproval after drafting recommendation, negotiating within framework to agreement

Sources: Texas Health Resources; Health Care IT Advisor research and analysis.
A Scalable Approach Without Complexity

UPMC$^1$ Susquehanna Pulls in the CMIO to Give Clinicians a Voice

UPMC Susquehanna Security Advisory Group
Convenes monthly and ad hoc to address critical issues

- Chief Legal Counsel + 1
- other legal representative
- Privacy Officer
- CTO
- CIO
- CMIO

• Reviews internal security communications
• Provides approval for various actions
• Vets security plans
• Addresses privacy-related issues related to security breaches
• Ensures security team listens to voices across the organization
• Considers physician workflow via CMIO representation

Case in Brief: UPMC Susquehanna

- Four-hospital non-profit integrated delivery system in north-central Pennsylvania; will be integrated into UPMC in the near future
- Physicians have been using biometrics since 2005 (fingerprints), 2-factor authentication, and “Tap and Go” badges
- Personal email is completely blocked on network
- Conducts simulated phishing attacks from which no one is exempt
- CISO reports to CTO who reports to CIO. CISO has dotted reporting line to CIO but meets regularly only with CTO
- CISO has a team of 2.5 security FTEs

1) UPMC = University of Pittsburgh Medical Center.

Sources: UPMC Susquehanna; Health Care IT Advisor research and analysis.
Security Officer Must Align with Entire Organization

CISOs Reporting to CEOs More Likely Outside of Health Care

Observed Organizational Models

<table>
<thead>
<tr>
<th>Degree of Centralization of Security Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Distributed</strong></td>
</tr>
<tr>
<td>Various functions spread across different areas</td>
</tr>
<tr>
<td><strong>Divided</strong></td>
</tr>
<tr>
<td>Security responsibilities split between IT and another administrative department such as compliance, legal, audit</td>
</tr>
<tr>
<td><strong>Centralized</strong></td>
</tr>
<tr>
<td>All security functions under one manager, the security officer</td>
</tr>
</tbody>
</table>

Key Considerations

*Must Match Security Culture and Goals of Your Organization*

- How mature is your security posture?
- How cyber-literate are your decision makers?
- What is your cultural approach toward security?
- To what degree do you want to change the security culture?
- How critical is innovation to your organization?
HCO CIO Sentiment Favors CISO Reporting to CIO, IT

Dotted Line Outside of IT a Possible Structure to Promote Transparency

Parkview Health’s Dual CISO Reporting Structure

Case in Brief: Parkview Health

- Non-profit, eight-hospital health system and medical group based in Fort Wayne, IN
- CIO and CISO lead a strong and consistent effort for transparency on cybersecurity issues
  - Dual reporting structure for CISO who can go to someone outside of IT if feeling things are going astray
- Information security presentations to multiple board committees annually, creating an environment in which several board members hear message multiple times
  - Standing agenda item on the Board IT Committee (quarterly); agenda item with Audit and Compliance committees

Aligned motivations amongst key leaders outperform official reporting structures.
Attract and Retain Talent with a Blame-Free Culture

It’s a Candidate’s Market: Culture, Authority, and Compensation Are Critical

CISO

17 months Average CISO tenure across all industries¹

Top Contributing Factors to CISO Turnover⁶

31% Lack of serious cybersecurity culture
30% Lack of active participation with executives
27% Offered higher compensation elsewhere

Case in Brief: Methodist Le Bonheur Healthcare

- Non-profit six-hospital system based in Memphis, TN
- Recognized by Fortune as one of the 100 Best Companies to Work For; #1 within Health IT category³
- Creates “stickiness for top talent” by focusing on highly responsive and supportive service to both patients and fellow associates

Security Personnel

1M Global cybersecurity openings in 2016²

Consider leveraging:
- Location
- Longevity
- Mission and purpose
- Career pathing options

Case in Brief: Inspira Health Network

- Non-profit three-hospital system based in Mullica Hill, NJ
- Security team of four FTEs⁴ leverages “as-a-service” for several security functions
- Partners with local universities for internships; half are dedicated to Rowan University with whom they have a formal arrangement
- Developed several key contributors from intern pool including on security, BI⁵ system programming teams

Source: Health Care IT Advisor interviews, research, and analysis.
Empower and Equip Your CISO for Success

“Exceptional Ones Possess a Combination of Skills Rarely Found in One Person”¹

Who You Put in the Role Matters

Technical Ability
- Exhibits a native curiosity about how things work

Leadership Skills
- Paints a clear and convincing vision of security without technical complexity
- Is a capable and level-headed leader in a crisis
- Sees negotiation as a necessary component for advancing security in the organization
- Gets things done through formal and informal channels

Business Savvy
- Approaches risk as an issue of degrees, not an absolute
- Understands business, clinical, legal, and regulatory implications
- Willingness to learn and adapt to the culture

Prepare Them for the Boardroom

Executive Mentor

Readies CISO for board-level executive discussion in a safe space
Refines language to exclude any confusing technical explanation
Provides opportunity to educate and develop an ally in the boardroom

From
I can prevent and eliminate all risk

To
I can mitigate organizational risk

Source: Health Care IT Advisor research and analysis.

CISO: The Corporate Rock Star of the Future?^1

Sample CISO Responsibilities for Job Description

**Risk Management**
- Work with organizational leaders to establish an acceptable level of risk for the enterprise
- Assess current security against this level of risk
- Develop strategy and implementation plan to ensure the enterprise achieves the acceptable level of risk
- Develop a security governance structure and process
- Ensure regular risk assessments are performed, and risks are tracked and corrected
- Manage vendor relationship and associated risk

**Technical**
- Lead identity and access management, user provisioning, and de-provisioning functions
- Lead incident response teams
- Lead investigations into security-related incidents and anomalous activity
- Ensure the development and maintenance of a resilient security architecture including consideration of such technologies as encryption, network access control, network access device, intrusion detection software, firewalls, anti-virus, VPN,^2 mobile device management software, etc.

**Policies and Procedures**
- Develop, review, enhance, and update all security-related policies and guidelines such as data classification, access control policies, data protection policies, staff security training policies, segregation of duties, data disposal and retention, password criteria, timeout requirements, user rights, etc.
- Responsible for disaster recovery and business continuity planning

**Compliance, Audit, and Legal**
- Understand, manage, and ensure compliance with legal, regulatory, and contractual requirements
- Work closely with internal and external audit, privacy officer, and compliance officer

**Leadership and Relationships**
- A well-qualified candidate will be comfortable working and communicating with executive and technical leadership around the company to embed a security-focused mindset in all areas
- Work closely with leaders in HR and IT functional areas to ensure security standards, policies, and procedures are deeply embedded and understood
- Lead security-focused culture and process change through training and interaction with department leaders

---


Source: Health Care IT Advisor research and analysis.
Virtual CISO: A Viable and Promising Option

HCOs with Limited Security Resources Can Leverage Security Experts

Case in Brief: NorthBay Healthcare

- Two-hospital health system with a 100+ physician medical group based in Fairfield, CA
- Outsource the majority of their security functions to a trusted vendor, Sword and Shield, to gain a depth of coverage likely unattainable with the current size of security team
- Virtual CISO reports to their Director of Network Operations, who functions as the official CISO for HIPAA
- Able to leverage specialized skills on the vendor side depending upon the needs of the specific question, project, or incident

Considerations for a Virtual CISO Model

Establish a Collaboration Approach

Take time to learn about each other and develop communication and report sharing patterns that meet the organization’s specific needs.

Set Clear Service Expectations from Start

Specify the scope of work and services and fine tune an agreement on the deliverables.

Identify a Main POC\(^1\) at the Vendor

Use a main POC to improve the vendor’s understanding of the organization’s culture, people, and processes. This will allow for better coordination of appropriate resources.

---

1) POC = Point of contact.

Sources: NorthBay HealthCare; Health Care IT Advisor research and analysis.
Digital Supply Chain Broadens Your Risk Exposure

Public Does Not Easily Discern Third-Party Breach Responsibility

Concerns Magnify with Third-Party Vendors

- Fourth- and n\textsuperscript{th}-party vendors, subcontractors
- Managed service providers, medical devices, hardware and software vendors, all vendor users with physical and network access
- External threats, staff and clinicians, mobile devices, shadow IT

49% Percent of respondents who have experienced a breach via a vendor\textsuperscript{1}

High-Profile Third-Party Breaches

- 40M customer debit and credit care accounts exposed
- Hackers entered via HVAC\textsuperscript{2} vendor with network access
- CIO and CEO resigned within a few months
- 15,000 patients had their data exposed on its transcription service vendor’s website
- BMC terminated their long-term relationship with MDF Transcription Services

\textsuperscript{1} Data Risk in the Third-Party Ecosystem, Ponemon Institute, April 2016.
\textsuperscript{2} HVAC = Heating, ventilation, and air conditioning.

Source: Health Care IT Advisor research and analysis.
BAAs¹ One Part of Third-Party Risk Management

Operational Issues to Be Clarified in Contract, BAA, or MOU²

Operational Considerations

• Patient record responsibility?
• Who will agree to indemnify whom?
• Risk assessments, audits, and sharing of results
• Policies:
  – Minimum required protections
  – Identity and access
  – Password policies
• When data is exchanged, what are the lifecycle terms?
  – Limitations on use
  – Disposal requirements
• Notification responsibility when a legitimate user’s role changes and access should be revoked
• SLAs³ around provisioning and de-provisioning

In Event of a Breach

• Who has the right of notification (to compromised parties, regulatory authorities, and the media)?
• Responsibility for notification (to compromised parties, regulatory authorities, and the media)?
• Approval authority over notifications?
• Covers the cost of notification?
• Notifies the media?
• Whose insurance covers what?
• Who pays for remediation (e.g., identity theft monitoring)
• Who conducts forensics?
• Who has the right to review results of forensics?

1) BAA = Business associate agreement.
2) MOU = Memorandum of understanding.
3) SLA = Service-level agreement.

Source: Health Care IT Advisor research and analysis.
### A Smart Approach to Third Parties: Trust, But Verify

**BAA’s Required for HIPAA, But Insufficient to Address Risk**

**Halifax Health’s Multi-Prong Third-Party Risk Management**

<table>
<thead>
<tr>
<th>Initial Third-Party Risk Review Process</th>
<th>Evaluation of Formal Outbound Data Transfers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Perform technical reviews</td>
<td>• Data governance council reviews all reports generated internally and sent to external parties</td>
</tr>
<tr>
<td>2. Evaluate vendors via a risk assessment and review process</td>
<td>• Involves multiple stakeholders across departments that exchange data with external entities including CQO, CMO, CCO, COO, CIO, CMIO, Finance, Patient Billing</td>
</tr>
<tr>
<td>3. Scan any hardware, devices, or software brought in to detect any vulnerabilities</td>
<td>• Have the authority to deny data sharing</td>
</tr>
<tr>
<td>4. Audit network access for third-party users, cutting off access as appropriate</td>
<td></td>
</tr>
</tbody>
</table>

**Security Team Philosophy**

- Security of patient data kept top of mind for all IT employees and Halifax Health management
- Third-party risk addressed on a daily basis

Sources: Halifax Health; Health Care IT Advisor research and analysis.
Business Models Are Changing; So Should Security

Mergers, Acquisitions, Alliances: HCOs Can’t Go It Alone Anymore

The Emergence of Value-Based Care

Volume-based care has led to seeking greater scale and lower costs by merging into holding companies.

These holding companies are transforming into operating companies to raise quality and lower costs via standardization.

Effective population management will ultimately drive the formation of more agile virtually integrated enterprises.

Autonomous

Holding Company
- Local autonomy
- High degree of heterogeneity in systems, processes
- Hospital-centric model

IT Architecture
Best of Breed/Distributed

Information Security
Each organization manages security; minimum standards and capabilities often vary

Synergistic

Operating Company
- Little or no autonomy
- Systems and process standardization
- Centralized services

IT Architecture
Enterprise Suite/Centralized

Information Security
Centrally managed to meet minimum requirements and have consistent policies

Agile

Virtually Integrated Enterprise
- Loosely coupled partners and affiliates but tightly integrated community of care
- Unifying strategy
- Pieces / parts can be rapidly reconfigured

IT Architecture
Extended Enterprise

Information Security
Relies on contractual agreement of minimum standards and regular reviews to ensure adherence

Source: Health Care IT Advisor research and analysis.
Set a Standard for Integration

Know Your Minimum Requirements; Assess Cyber Risk of Any Relationship

Case in Brief: Atlantic Health System

- Five-hospital system including a 600-provider medical group based in Morristown, NJ
  - Member of AllSpire Health Partners—alliance of seven hospital systems focused on quality, PHM,¹ best practices, and medical research in the Northeast region
- Established a standard 36-month IT practice for integrating acquired organizations
- When an organization is acquired, a third-party security assessment is conducted to determine compatibilities and identify areas of challenge
- Networks and email are not merged until IT standards are met
  - Leverages techniques like Virtual Desktop Infrastructure as a bridge solution

Lessons Learned

Establish a standard approach for IT integration prioritizing information security

Assess before integration

Define upfront what is mandatory but offer flexibility on the rest

Provide toolkit of bridge solutions until minimum requirements are met

Consider switching costs before forcing a change

¹ PHM = Population health management.

Sources: Atlantic Health System; Health Care IT Advisor research and analysis.
Establish a Standard Roadmap That Prioritizes Security

Sequence IT Changes and Prioritize Security: Atlantic Health Example

"Standard but flexible—this represents the integration process we aim for, but it depends on what the other guy is willing and able to do."

Linda Reed
Former VP, CIO
Atlantic Health System

1) HR = Human Resources; 2) PACU = Post-Anesthesia Care Unit; 3) RIS = Radiology Information System; 4) PACS = Picture Archiving and Communications System; 5) CPOE = Computerized Provider Order Entry; 6) OB = Obstetrics.

Source: Reed L, “IT Realities of Health System Integration,” CHIME 2014 Fall Forum presentation.
Relevant Opportunity Areas for Senior Leadership

Governance and Policy
- C-Suite and Board Engagement
- Dashboards
- Governance Standards
- Strategy
- Digital Trading Partners
- Staffing

Cyber Resilient Organizations

Process and Education
- Training
- Testing
- Incident Response Planning
- Audits
- Business Continuity Planning + Back-ups + Disaster Recovery
- Risk Assessments

Technology and Services
- Cyber Intelligence
- IT-Enabled Capabilities
- Cyber Insurance
- Information Sharing

Source: Health Care IT Advisor research and analysis.
The Human Firewall: Training Alone Is Not Enough

HCOs Must Validate That Users Understand and Apply Learnings

Continuous and Applicable Awareness Training

- Focus training on current higher risks using real examples and the latest techniques
- Think bite-size: don’t try to cover everything at once
- Personalize training to roles, making it fun and engaging, but not ridiculous
- Leverage multiple communication channels
- Provide easy-to-find materials on FAQs,¹ contact information, including “what to do if…”
- Engage front-line management and departmental leadership to support and reinforce processes

User Click Decision

Continuous Testing and Validation

- Test all users with email privileges, regardless of seniority or role
- Use the latest scammer techniques
- Leverage cyber intelligence and simulations for social engineering
- Test against multiple communication channels (email, text, phone), entry ways (e.g., dropped USB in parking lot), and physical access points (e.g., badge tailgating)
- Track and share performance
- Consider what type of accountability your organization is willing to enforce

¹ FAQs = Frequently asked questions.
Involve Executive Leadership in Phishing Campaigns

Harness Valuable Teaching Moments When They Present Themselves

C-Suite Involvement in Internal Phishing Campaigns

What is the best cultural fit for your organization?

Excluded or pushing back

Included, exempt from remediation

Committed to participation

Involved in process

Vocal advocate

Metro Health

- C-suite supportive of internal phishing campaigns
- C-suite signs pledge to complete the remediation training if caught

Eastern Maine Healthcare System

- Chiefs of HR, Legal Counsel chose a campaign—“click here to confirm your merit increase”
- Able to diffuse push back

Parkview Health

- C-suite included in every internal phishing campaign
- Prominent board member clicked, then admitted it to the entire board for all to learn from the error

Everyone is susceptible

Source: Health Care IT Advisor interviews, research, and analysis.
Visible Results Can Motivate and Promote Awareness

But Only If You Hold C-Suite Attention and Link Results to Desired Behaviors

Facility-Level Click Rates Shared During Regular Monthly Call

- 9% Facility 1
- 5% Facility 2
- 12% Facility 3
- 22% Facility 4

Flexible and Scalable Gamification Options

- **Employee-Level**
  - Individuals or self-selected teams (similar to step count competitions)

- **Department-Level**
  - Department or work function across the enterprise or by team with department

- **Executive-Level**
  - Executives by facility or region across the enterprise or by top executive for each work function

Case in Brief: RCCH Healthcare Partners

- For-profit health system of 17 hospitals in 13 states, headquartered in Brentwood, TN
- All facilities are phished once per month with socially engineered “bait”
- CIO shares facility-level click rate performance with facility CEO leadership during regular monthly call
- Remediation training auto-triggered for those who inappropriately clicked
- Personal email services blocked on networks

Source: Health Care IT Advisor interviews, research, and analysis.

1) Sample data depiction.

©2018 Advisory Board • All Rights Reserved • advisory.com • 35132G
Gamification Embeds Security Within Culture

Even Simple Games with Rewards for Key Behaviors Can Be Effective

Steps to a Gamified Security Awareness Program

1. **Define and Prioritize Key Behaviors**
   
   Key behaviors should link to your desired results and improvements; determine how you will measure results

2. **Build and Roll Out Program**
   
   Establish executive buy-in; connect efforts to a purpose, allow discretionary participation; establish motivational reward system; determine duration of program; communicate expected behaviors

3. **Test and Give Feedback**
   
   Verify player actions providing opportunities for players to illustrate positive behaviors; measure progress in key behaviors

4. **Reward and Recognize (or Educate)**
   
   Communicate standings; use a leaderboard that engages across the standing (not just the top 10%); supply motivational rewards or incentives; educate with remedial training as needed

5. **Foster a Social Connection**
   
   Leverage a social network to answer questions, interact with players, acknowledge leaders, promote or reinforce interest in the program

---

**Case in Brief: Salesforce**

- Leading cloud-based customer relationship platform headquartered in San Francisco, CA
- Highly gamified approach to security awareness that is deeply embedded in workforce culture
- Two points-type system:
  - Trust points reflect security championship level (an aggregate of all points ever earned)
  - Smart points can be spent for prizes
- Use Chatter to provide quick reaction to security questions and recognize participants who demonstrate positive behaviors

---

Salesforce’s Advanced Security Behavior Gamification

Program Transformed Security Behaviors from “Have to” to “Want to”

Salesforce Security Champion Program
Players move upwards by accruing trust points

How to Earn Trust Points
Selection of Salesforce’s actions and trust point values

<table>
<thead>
<tr>
<th>Positive Behavior or Action</th>
<th>Trust Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive a Trust badge</td>
<td>50</td>
</tr>
<tr>
<td>Read security newsletter and chatter about it</td>
<td>50</td>
</tr>
<tr>
<td>Report phishing email / social engineering call</td>
<td>100</td>
</tr>
<tr>
<td>Complete 100-level security awareness course</td>
<td>100</td>
</tr>
<tr>
<td>Complete 200 or 300 level security awareness course</td>
<td>200</td>
</tr>
<tr>
<td>Attending a security lunch and learn</td>
<td>200</td>
</tr>
<tr>
<td>Win a “Bug Bounty” event</td>
<td>500</td>
</tr>
<tr>
<td>Attending a hands-on security training course</td>
<td>600</td>
</tr>
<tr>
<td>Teaching or presenting on a security topic</td>
<td>1,000</td>
</tr>
</tbody>
</table>

Reward Structure Depends Upon Culture

- C-suite must be willing to support
- Rewards can include executive or C-level recognition, certificates, status, badges, t-shirts, gift cards, time off
- Prizes can promote teamwork (e.g., free lunch for department)
- Prizes should make the efforts worth it!

Sample of Security Behaviors to Incentivize for Provider Organizations

- Stop a badge surfer
- Read security newsletter or article and pass a quiz
- Report phishing email (internal or actual)
- Report a social engineering call
- Turn in a USB dropped in the parking lot
- Complete various levels of security awareness training
- Attend a security lunch and learn
- Pass monthly or quarterly security quizzes
Build from Strong CMIO Relationship with Clinicians

Compromise on Both Sides Will Be Necessary

“If the computer let’s me do it, it must be ok.”

Common physician and nurse mindset

The CMIO takes my Romulun and makes it decipherable.”

Ron Mehring, CISO
Texas Health Resources

Develop

• Consult with CMIO, CNIO, CMO, CNO, physician and nurse leadership
• Negotiate policies, processes, and investments with key clinical leaders to come to appropriate compromise

Operationalize

• Test how well policies, processes, instructions, workflows work for clinicians in an informal “lab” using sample of clinicians
• Pilot with clinicians, if possible, incorporating feedback
• Fine tune trainings or materials to be efficient and worthwhile for clinicians

Promote and React

• Partner with CMIO, CHIO, CNIO to:
  – Present any security changes and workflow impacts to physician leadership
  – Introduce security changes with language that resonates
  – Lobby one-on-one with holdouts
• Use physician and nurse leadership to deliver bite-sized communications
• Round to observe, collect feedback

Opportunity to Educate, Communicate, and Build Clinician Buy-in and Trust

Clinician Impact

If the computer let’s me do it, it must be ok.”

Common physician and nurse mindset

The CMIO takes my Romulun and makes it decipherable.”

Ron Mehring, CISO
Texas Health Resources
What Type of Accountability Will You Enforce?

Human Resources and Legal Must Support and Enforce Policy

Spectrum of Accountability

- **No Fault**
  - Learning opportunity

- **Performance Review**
  - Component of or tied to review or merit increase

- **Progressive Discipline**
  - Counts as any other violation of firm policy

- **Three Strikes**
  - Revokes external email privileges with third strike

- **Tiered Reprimand**
  - Based upon the severity of the violation of trust

### Key Questions

- How do you define “repeat offender”?
- How do you handle a repeat offender? What if he/she is a physician?
- Can you codify it in firm policy?
- What can you do to proactively avoid some of these situations?
- Does the accountability structure fit the culture of the organization?
- Do you have a strong partnership with HR, Legal, and Compliance executives to support and enforce these policies?

### Case in Brief: UPMC Susquehanna

- Four-hospital health system based in Williamsport, PA
- Eliminated external email for 600 nursing staff in response to phishing campaign for individuals who did not require external email for their role
- Staff still receive manager communications, information regarding benefits, and other internal emails
- May revoke external email privileges for repeat-offender physicians
- Use KnowBe4’s PhishAlert Outlook plugin to promote quick and easy reporting of suspected phishing attempts

Source: Health Care IT Advisor interviews, research, and analysis.
Relevant Opportunity Areas for Senior Leadership

Technology and Services

Governance and Policy
- C-Suite and Board Engagement
- Governance Standards
- Strategy
- Digital Trading Partners
- Staffing

Cyber Resilient Organizations

Process and Education
- Training
- Testing
- Incident Response Planning
- Audits
- Business Continuity Planning + Back-ups + Disaster Recovery
- Risk Assessments

Technology and Services
- Cyber Intelligence
- IT-Enabled Capabilities
- Cyber Insurance
- Information Sharing

Source: Health Care IT Advisor research and analysis.
Wild West of Security Vendors

Prepare Your C-Suite for What to Look Out for in Security Messaging

$10.9B
Estimated size of global health care cybersecurity market in 2022

$29B
Estimated size of global Internet of Things cybersecurity market in 2020

$8.5B
Estimated size of security-as-a-service market by 2020 with health care as the largest market

$170B
Estimated size of global cybersecurity market in 2020

Use Data to Show How Security Layers Work Together

From 800K Malicious Emails to Zero Users at Risk

Six Layers of Protection Result in High Reliability at Texas Health Resources

12M Total External Emails

1st Level Email Filtering
- 779,275 malicious emails
- 3,402 emails delivered
- 2,034 users at risk

2nd Level Email Filtering
- Website Link Re-Write
- 1,930 users at risk

User Training
- 12 users at risk

Web Gateway Blocking Uncategorised Websites
- 1 user at risk

Endpoint Malware Protection
- 0 users at risk

Highlights necessity of a layered approach to security defenses

Illustrates an impact of technical and human training investments

Quantifies reduction in risk for a data-based conversation

Connects security to a broader organizational strategy

Sources: Texas Health Resources; Health Care IT Advisor research and analysis.
1. Current State of Security Affairs

2. How IT and Non-IT Leaders Can Drive Cyber-Resiliency

3. The Long Game: A Path Toward an Adaptive Security Posture
## Summarized Cybersecurity Maturity Model

<table>
<thead>
<tr>
<th>Governance and Policy</th>
<th>Basic</th>
<th>Automated</th>
<th>Adaptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership engagement, governance, standards, strategy, staffing, legal, digital trading partners</td>
<td>Leadership views security as someone else’s problem</td>
<td>Partial but growing leadership engagement and support</td>
<td>All leaders clear on roles</td>
</tr>
<tr>
<td></td>
<td>Little or no use of security standards</td>
<td>Limited use of standards</td>
<td>Leadership dashboard</td>
</tr>
<tr>
<td></td>
<td>No documented security strategy</td>
<td>Defense-in-depth strategy documented but no roadmap</td>
<td>Full adherence to standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Adaptive strategy documented and progress actively tracked</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process and Education</th>
<th>Basic</th>
<th>Automated</th>
<th>Adaptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training, testing, incident response plan (IRP), risk assessment, audits, business continuity planning (BCP), disaster recovery (DR)</td>
<td>Annual training, minimal to no testing with pushback</td>
<td>Mandatory training and testing</td>
<td>Continuous training via multiple tools</td>
</tr>
<tr>
<td></td>
<td>Basic IRP never or rarely tested</td>
<td>IRP includes templates and pre-vetted service providers</td>
<td>Phishing campaigns driven by cyber intel</td>
</tr>
<tr>
<td></td>
<td>Annual risk assessments</td>
<td>Quarterly risk assessments</td>
<td>Risk assessments aligned with change management</td>
</tr>
<tr>
<td></td>
<td>Auditors, security, and IT track issues separately</td>
<td>Central issue tracking</td>
<td>Auditors, security, and IT aligned</td>
</tr>
<tr>
<td></td>
<td>Little or no BCP; and DR infrequently tested</td>
<td>BCP documented and DR tested regularly</td>
<td>Regularly tested BCP and DR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology and Services</th>
<th>Basic</th>
<th>Automated</th>
<th>Adaptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and access management (IAM), cyber intelligence, cyber insurance, information sharing, mobile device management (MDM)</td>
<td>Technical basics: Firewalls, intrusion detection, web and email filters, anti-virus software</td>
<td>More advanced tools</td>
<td>Proactive stance</td>
</tr>
<tr>
<td></td>
<td>Manual IAM</td>
<td>Multiple IAM tools</td>
<td>Self-service IAM</td>
</tr>
<tr>
<td></td>
<td>Manual cyber intelligence</td>
<td>Intrusion detection and response system (IDRS)</td>
<td>SIEM²</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber intelligence service</td>
<td>Active cyber intelligence service leveraging AI¹</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MDM and network access controls deployed</td>
<td>Regular pen testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber insurance</td>
<td>Network segmentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dynamic access control</td>
</tr>
</tbody>
</table>

1) SIEM = Security incident and event management.
2) AI = Artificial intelligence.

Source: Health Care IT Advisor research and analysis.
The Start of the Journey

Good Raw Materials, But Miles to Go for C-Suite, Clinician Engagement

Governance and Policy
- Immature governance and policies, building a roadmap
- Strong alignment across finance, compliance, and IT
- Board interested, but roles still need to be defined

Process and Education
- Significant push back from C-suite on internal phishing campaigns
- Clinical staff resistant to drilling on downtime procedures

Technology and Services
- Technology basics are in place
- Interest in as-a-service options to build in more robust capabilities without adding staff

Case in Brief: Pineland Health Care

- Community hospital and medical group located in the Southeast
- Current CIO is the first IT executive for the organization and has cultivated strong relationships with fellow executives, including the board
- Divided CISO responsibilities between CIO and security engineer
- IT team is highly customer focused
- Initial cyber education efforts have been well received by the board, but are infrequent

1) Pseudonym.
Maturing Security Across the Organization

Culture Approaches Patient Data, Security as a Patient Safety Issue

**Governance and Policy**
- Executives think of patient data as a patient safety issue
- CIO articulates clear security and IT vision to executives and department
- Eliminated use of technical terms outside of IT department

**Process and Education**
- Education efforts equate good cyber hygiene to caring for patients
- Frequent testing of DR and BCP for downtime procedures

**Technology and Services**
- Advanced technologies in place

---

**Case in Brief: Halifax Health**
- Two-hospital health system based in Daytona Beach, FL
- Consistently tie security efforts to patient safety and patient care
- Tight partnership with General Counsel and CIO, especially around contractual agreements that may involve IT or have security implications
- Repeat offenders in an ongoing, random selection phishing campaign lose Outlook until education is completed; education may include one-on-one meetings with CIO or IT Security Risk Manager for hands-on training

Sources: Halifax Health; Health Care IT Advisor research and analysis.
Long-Term Dedication to Cyber Resiliency

Adjusts to the Changes in the Enterprise and the Threat Landscape

Governance and Policy

- Mature and centralized security program governance
- Organizational risk approach
- Emphasis on collaboration
- Long-term leadership and organizational commitment to cybersecurity

Process and Education

- Strong partnership with CMIO, CHIO, CNIO leadership for clinician engagement efforts
- Connects security efforts to “High Reliability Organization” strategy and “Living Our Promise” initiative

Technology and Services

- Proactive stance with identification of trends through analytics
- Advanced threat detection program in place

Case in Brief: Texas Health Resources

- Faith-based, non-profit 24-hospital health system based in Arlington, TX
- Highly-centralized security program across all facilities to ensure consistency
- Consultative security governance structure with executive representation from across the organization involved in defining security parameters and frameworks
- Frequent negotiations to strike the right balance between security and end-user needs
- Facilitate strong horizontal peer relationships within mid-level management to buy into, promote, and reinforce security procedures

Sources: Texas Health Resources; Health Care IT Advisor research and analysis.
# Technology-Enabled Capabilities for Cyber C-Suites

<table>
<thead>
<tr>
<th>Threat</th>
<th>Essential</th>
<th>Nice to Have</th>
<th>Future Need</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lost or Stolen Device</strong></td>
<td>• Encryption</td>
<td>• Virtual Desktop Infrastructure (VDI)</td>
<td>• Biometrics</td>
</tr>
<tr>
<td></td>
<td>• Mobile Device Management (MDM) Container</td>
<td>• Data Loss Prevention</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Card Key Locks</td>
<td>• Lowjack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Awareness Training</td>
<td>• MDM Kill Pill</td>
<td></td>
</tr>
<tr>
<td><strong>Insider Abuse</strong></td>
<td>• Audit Logs</td>
<td>• Threat Intelligence Service</td>
<td>• Segmentation</td>
</tr>
<tr>
<td></td>
<td>• Policy Enforcement</td>
<td>• Usage Monitoring</td>
<td>• Security Analytics</td>
</tr>
<tr>
<td></td>
<td>• Awareness Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phishing/Social Engineering</strong></td>
<td>• Web and Email Filters</td>
<td>• Threat Intelligence Service</td>
<td>• AI-enabled Security Analytics</td>
</tr>
<tr>
<td></td>
<td>• Anti-virus Software</td>
<td>• White Listing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Business Continuity/Disaster Recovery</td>
<td>• Awareness Testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Awareness Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Probing</strong></td>
<td>• Firewall</td>
<td>• Threat Intelligence Service</td>
<td>• Honeypots</td>
</tr>
<tr>
<td></td>
<td>• Intrusion Detection System (IDS)</td>
<td>• Penetration Testing</td>
<td>• Security Information and Event Management (SIEM)</td>
</tr>
<tr>
<td></td>
<td>• Patch Management</td>
<td>• Multi-factor Authentication</td>
<td>• Single Sign-on</td>
</tr>
<tr>
<td></td>
<td>• Incident Response</td>
<td></td>
<td>• Security Analytics</td>
</tr>
<tr>
<td></td>
<td>• Awareness Training</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key Takeaways for Cyber C-Suites

Cyber Resilience Demands Focus on Partnerships, Culture, and Layers

1 **Forge and maintain critical partnerships across the C-suite**
   Strong and effective partnerships between IT and security leaders with individuals inside and outside of the C-suite and boardroom are essential to drive organization-wide cyber preparation efforts.

2 **Explore ways leadership can promote a security-focused culture**
   While typically focused on funding technological defenses, executive leadership has significant opportunity to promote a cybersecurity-focused culture through their support and buy-in of other components of the cybersecurity ecosystem.

3 **Build cyber-resilience through layers**
   True cyber resilience comes when organizations master all elements of the cybersecurity ecosystem, including governance and policy, process and education, and technology and services.

4 **Leverage this research material to continue your C-suite engagement efforts**
   Use this content in those private conversations; let us know how the Advisory Board can support your efforts (private web conferences, workshops, facilitated discussions, on-sites with executives, etc.).

Source: Health Care IT Advisor interviews and analysis.
Paint a Picture of a Cyber-Resilient Organization

Appendix—Additional Resources

Infographic: Critical IT Leader Actions and Non-IT Leader Lessons

When a Breach Occurs, the Whole Hospital Is Our Patient

Infographic: Engage Clinicians in Cybersecurity Conversations