The Five Pillars of a Best-in-Class Cybersecurity Program
Session 90, March 6, 2018

Kevin Charest
Divisional Senior Vice President and Chief Information Security Officer

Himss18 The leading health information and technology conference
WHERE THE WORLD CONNECTS FOR HEALTH
Conference & Exhibition | March 5–9, 2018
Las Vegas | Venetian – Palazzo – Sands Expo Center

COMMITMENT

www.himssconference.org

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.
Conflict of Interest

Kevin Charest, PhD

Has no real or apparent conflicts of interest to report.
Agenda

• Introductions
• Background on Health Care Service Corporation’s cybersecurity program
• Five pillars of a best-in-class cybersecurity program
• Implementing your cybersecurity program
• Q&A session
Kevin Charest

• Divisional Senior Vice President and Chief Information Security Officer at Health Care Service Corporation
• Vice President of IT Security and Cyber Defense Operations at UnitedHealth Group
• Chief Information Security Officer for the Department of Health and Human Services
• Board Chair of The International Information System Security Certification Consortium (ISC)²
# Learning Objectives

| 1 | Identify the five pillars of a best-in-class cybersecurity program |
| 2 | Identify challenges and barriers to overcome when building a cybersecurity program |
| 3 | Assess an existing cybersecurity program to identify improvements |
| 4 | Determine a course of action to improve an existing cybersecurity program |
| 5 | Measure the effectiveness of a cybersecurity program |
80+ Years of Success and Tradition

#6 on Diversity MBA’s 50 Out Front for Diversity Leadership Best Places to Work for Women & Diverse Managers

15 million members

Operating health insurance plans in FIVE states: IL, MT, NM, OK, TX

Over 21,000 employees

208.3 million claims processed annually

LARGEST customer-owned health insurer in the U.S. and 4th largest overall

Our Purpose

To do everything in our power to stand with our members in sickness and in health®

1936 year founded

2,100 IT employees

+$1 billion in IT spend
HCSC Cybersecurity Program

• Cybersecurity must move at the speed of the business
• Digital transformation is forcing evolution in cybersecurity programs and HCSC is at the forefront
• HCSC has a fully integrated cybersecurity program that enables and protects business innovation
The information security function must deal with the emergence of the digital operating model and its agile business driven approach to the market.

ENGAGE THE BUSINESS
- Be a trusted advisor to the business with a seat at the table
- Help guide investment decisions with security insight derived from robust metrics
- Offer simple and transparent services to increase coverage
- Develop solutions with clear traceability to business objectives

DELIVER RESULTS
- Decrease time to market for new security solutions
- Increase security consistency through enterprise-wide solution development
- Offer affordable services through reusable patterns and tiered engagement
- Establish clean hand-offs and accountability

IMPROVE CONTINUOUSLY
- Perform continuous and holistic security assessment and gap remediation to ensure quality
- Manage demand to improve agility and scale appropriately
- Take innovative approach to solving enterprise and industry wide problems
- Enable the growth and mobility of our people
So what’s in a cybersecurity program?

BEST-IN-CLASS CYBERSECURITY PROGRAM

- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement
Governance, Risk, and Compliance
Set forth the organization’s security strategy and enable governance functions to manage security risk.

Security Architecture and Engineering
Design, architect and engineer security solutions to protect the enterprise from known and potential risks and threats.

Information Security Operations
Manage and operate security solutions to help detect security vulnerabilities and events which pose risk to the enterprise.

Cyber Defense Operations
Respond, investigate and remediate incidents and potential breaches while enhancing architecture and operations through continuous feedback.

Business Engagement
Incorporate cybersecurity into everyday business decisions, processes and interactions with the customer.
So what’s in a Cybersecurity Program?

BEST-IN-CLASS CYBERSECURITY PROGRAM

- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement
Security Management & IT Risk Management

IT RISK Domains

- Cyber Security Risk
- Legal, Regulatory and Contractual Risk
- Third-Party and Subsidiary Risk
- IT Strategy Risk
- Information Security and Governance Risk
- IT Operations Risk

BEST-IN-CLASS CYBERSECURITY PROGRAM
Security Management & Risk IT Policy & Governance

• IT Policy & Governance
  Policies need to evolve to address changing risks in the IT environment

• Security Training & Awareness
  Specialized training (privileged, developer)
  Gamification
  Phishing
  IS website redesign

• Benchmarking Program Effectiveness
  Information Risk Executive Council (IREC)
Security Management & Risk IT Business Resiliency

- **Business Resiliency & Crisis Management**
  - Ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand reputation

- **Business Resiliency Components**
  - Enterprise Business Impact Assessment (BIA)
  - Business Resiliency Governance
  - Business Resiliency Planning
  - Business Resiliency Exercises

- **BR/DR Repository**
  - Centralization and Integration
BEST-IN-CLASS CYBERSECURITY PROGRAM

- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement
Enterprise Security Architecture

**PURPOSE**

Enable trusted, best-in-class services for customers by designing a robust and resilient ecosystem for service innovation and delivery.

**GOVERNANCE**

- Trusted, Risk-Balanced Digital Ecosystem
- Enterprise-Class Security Services
Cybersecurity Engineering – What We Do

Build and enhance technical security investments, ensuring expected business value and risk reduction is achieved. This is done by delivering in an agile manner to establish solutions that are resilient, flexible, and efficient.

**Training & Communication**

- Stakeholder Analysis & Communications Plan, Training Plan & Guides, Service Desk Scripts

**Capability Development Process**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Design</th>
<th>Build</th>
<th>Test</th>
<th>Deploy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements Documents</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review architectural use cases, functional and non-functional requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Technical and Infrastructure Design Docs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Plan &amp; Cases</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure provisioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAT, L&amp;T, regression, system testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational runbooks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Results Documented</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration catalog updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production cutover</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete Ops Handoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final reviews, signoff and warranty</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Standards Development

Ensure the confidentiality, integrity and availability of HCSC’s data and environments across on-premise, off-premise and cloud environments through standardization and automation.

- **RISK MITIGATION**
  Changing threat landscape with new players (e.g. governmental agencies)

- **TECHNOLOGY**
  Rapid pace of innovation

- **DECENTRALIZATION**
  Multi-vendor, multi-cloud strategy

- **INDUSTRY**
  Lean healthcare payer startups leading to disruption

- **REGULATORY COMPLIANCE**
  Shifts in regulatory compliance and legislation
Security Design & Architecture

Aligning security design, architecture and standards development in a continuous process that delivers secure computing platforms and services in support of strategic business initiatives.
BEST-IN-CLASS CYBERSECURITY PROGRAM

- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement
Information Security Operations

• In-house, out-sourced, or hybrid approach
• Platform management
• Operational processes and standards enforcement
• Threat and vulnerability lifecycle management
• Operational metrics
Management and Metrics are influenced by all of these factors.
BEST-IN-CLASS CYBERSECURITY PROGRAM

- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement
Cyber Defense Operations
The health care industry is under attack

According to the Identity Theft Resource Center, cyber attacks were the leading cause of data breach incidents for the eighth year in succession, accounting for 55.5 percent of the overall number of breaches in 2016, with 145 successful cyber attacks targeting health care.

Anthem data breach cost likely to smash $100 million barrier
The company’s cyber insurance policy is likely to be exhausted following the theft of up to 80 million records.

FierceHealthcare
CareFirst data breach ruling increases liability risks for insurers in future lawsuits

HealthData Management
OCR hits Memorial Healthcare System with $5.5M fine

Premera negligent in data breach, 5 lawsuits claim
Originally published March 27, 2015 at 8:18 pm
Cyber Defense Operations
Evolving Threat Landscape

• The world has changed. It is not what it was a decade or even 2 or 3 years ago.
• We are defending our members on the front lines of a rapidly evolving cyber threat landscape.
• Cybersecurity isn’t a black and white notion of “secure” or “not secure” but rather a constant state of the gray area in the middle.

Powerful Adversaries

The healthcare industry is facing threats we have never seen before as sophisticated nation-state attacks replace rogue hackers.

Significant Impact

Massive breaches exposing millions of personal records have shattered consumer confidence and brought cybersecurity into the spotlight.
Cyber Defense Operations
Adopting Assume Breach Methodology

We adopted this methodology to demonstrate the tactics and impact of an advanced threat. This approach enables us to realize the benefit of a breach simulation to measure our cyber defense capabilities.

Assumed Breach

Cyber breach is a case of “when” not “if”.

The Advanced Threat Simulation assumes a threat has penetrated the network and can established an initial foothold.

Assumed Click

People cannot be controlled and are susceptible to attacks that result in a compromise of their access.

The Simulation assumes an attacker can gain execution on an endpoint.

Incremental Sophistication

Advanced threats are profit oriented and will use the minimum sophistication required to breach a target.

Testing activities are performed to determine the minimum amount of complexity required to bypass a given security control.
Cyber Defense Operations Adversarial Simulation

The purpose of Adversarial Simulation is to test the effectiveness of enterprise security controls when confronted with a targeted advanced threat using varying levels of sophistication. The simulation is performed to assist in the prioritization of security controls that can consistently identify and mitigate the impact of an advanced threat.

Adversarial simulation assesses enterprise ability to:

**DEFEND**
- Restrict pivots through host based security tools and system hardening
- Restrict lateral movement with network segmentation and choke points

**DETECT**
- Identify activity through security tools or system event logs
- Correlate malicious activities across the enterprise
- Identify anomalous or abnormal use of accounts and systems

**RESPOND**
- Properly escalate and triage
- Quarantine the compromise area or network
- Prevent exfiltration of data
- Eradicate the threat and resume normal business operation

"the process of safely “attacking” a network from the outside in — as a hacker would — has become a must-have for health care organizations."
- Larry Pesce, Pauldotcom Security Weekly
Cyber Defense & Investigation
Assume Breach Detection & Response Capabilities

- Threat Actors
- Adversary Cyber Attack
- Advance Threat Analysis (ATA)
- Proactive Threat Hunting
- Cyber Kill Chain
- Persistence
- Privilege Escalation
- Credential Access
- Hard Enumeration
- Defense Evasion
- Lateral Movement
- Exfiltration
- Command and Control
- Calibration

Incident Response (IR)
Develops, maintains incident response activities, plans

Digital Forensics Service (DFS)
Computer, Network, Malware Forensics

24x7 Security Incident Detection and Monitoring (SiD&M)

Galvanic
Threat Intelligence Platform

TTP Defense Matrix
PUBLIC
LOCAL
HCSC
INTERNAL
ISAC
Security Big Data Lake
BEST-IN-CLASS CYBERSECURITY PROGRAM

- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement
Business Engagement

Incorporate cybersecurity into everyday business decisions, processes and interactions with the customer

- Checks & balance between security management & all other groups
- Understand the customer needs
- Feedback to IT & business groups
- Leverage Ops resources to implement solutions

FRAMEWORK

- Business & Customer Enablement
- Security Management & Risk
- Security Design & Architecture
- Security Operations
Business Engagement
Business Information Security Liaison

OVERVIEW

Improve the relationship with the business portfolios to understand their strategy, processes, approach and strengthen the enterprise security posture.

KEY ACTIVITIES

1. Connect the business to security to define and implement key investments
2. Educate the business on security capabilities, standards and policies
3. Provide business feedback into IS services, processes and capabilities for improvement
4. Empower the business to make the correct business decisions under the guidance of the BISOs
5. Anticipate and predict security needs and engage for remediation
Roadmap to Building a Cybersecurity Program

1. Create Strategic Plan
2. Cybersecurity Program Assessment
3. Create Prioritized Tactical Plan
4. Begin execution on people, process, & technology plan
5. Continuous Improvement
6. Address the gaps
7. Validate appropriate talent mix
8. Cybersecurity Program Maturity Assessment
9. Third Party Adversarial Test
10. Enhance strategic plan

Year 1

Year 2

Year 3
Questions?

Kevin Charest

- Kevin M Charest@hcsc.net
- Kevin Charest, PhD

HCSC
Health Care Service Corporation

Health Care Service Corporation, a Mutual Legal Reserve Company

Make sure to complete online session evaluation. Thank you!
Appendix
Governance, Risk, and Compliance
Set forth the organization’s security strategy and enable governance functions to manage security risk.

Security Architecture and Engineering
Design, architect and engineer security solutions to protect the enterprise from known and potential risks and threats.

Information Security Operations
Manage and operate security solutions to help detect security vulnerabilities and events which pose risk to the enterprise.

Cyber Defense Operations
Respond, investigate and remediate incidents and potential breaches while enhancing architecture and operations through continuous feedback.

Business and IT Liaison
Incorporate cybersecurity into everyday business decisions, processes and interactions with the customer.

Cybersecurity Strategy
IT Policy and Governance
IT Risk Management
IT GRC Controls
IT Business Resiliency

Security Architecture
Security Engineering
Security Standards

Platform Management
IS Processes and Tools
IS Threat and Vulnerability Management
IS Metrics and Reporting
Identity and Access Management

Security Big Data Lake
Cyber Fusion Center (SOC)
Red Team
Blue Team
Cyber Forensics and Incident Response

IS Intake and Demand