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

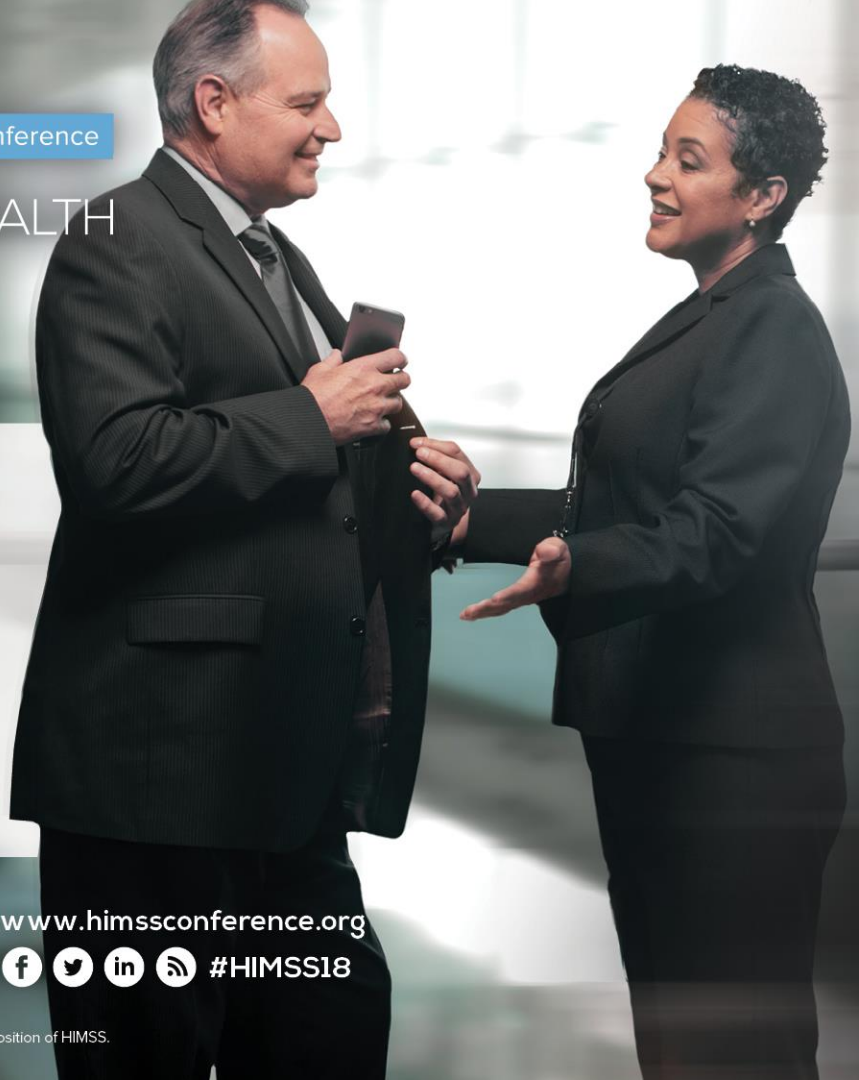
The Five Pillars of a

Best-in-Class Cybersecurity Program

Session 90, March 6, 2018

Kevin Charest
Divisional Senior Vice President and
Chief Information Security Officer

HCSC
Health Care Service Corporation



COMMITMENT

www.himssconference.org

#HIMSS18

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.

#HIMSS18
©HIMSS 2018

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

#HIMSS18
©HIMSS 2018

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

#HIMSS18
©HIMSS 2018

80+ Years of Success and Tradition

15 million members

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

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

Over **21,000** employees

+$1 billion in IT spend

Our Purpose

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

208.3 million claims processed annually

2,100 IT employees

1936 year founded

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

#HIMSS18
©HIMSS 2018

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

#HIMSS18
©HIMSS 2018

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

©HIMSS 2018

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

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)

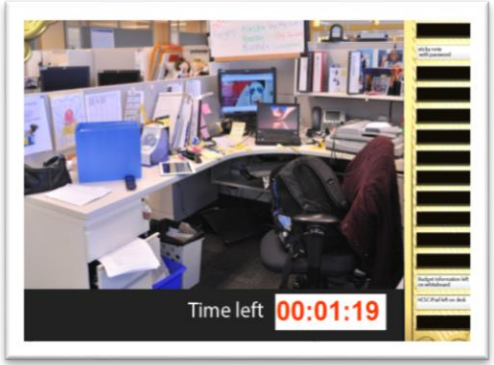
  Gamification

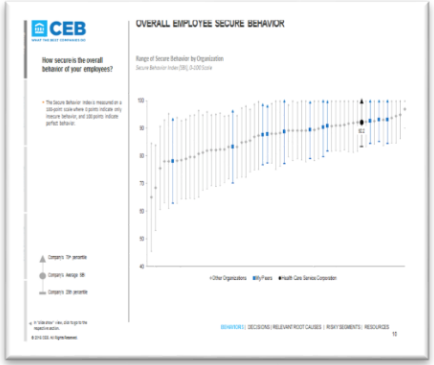
  Phishing

  IS website redesign

- **Benchmarking Program Effectiveness**

  Information Risk Executive Council (IREC)

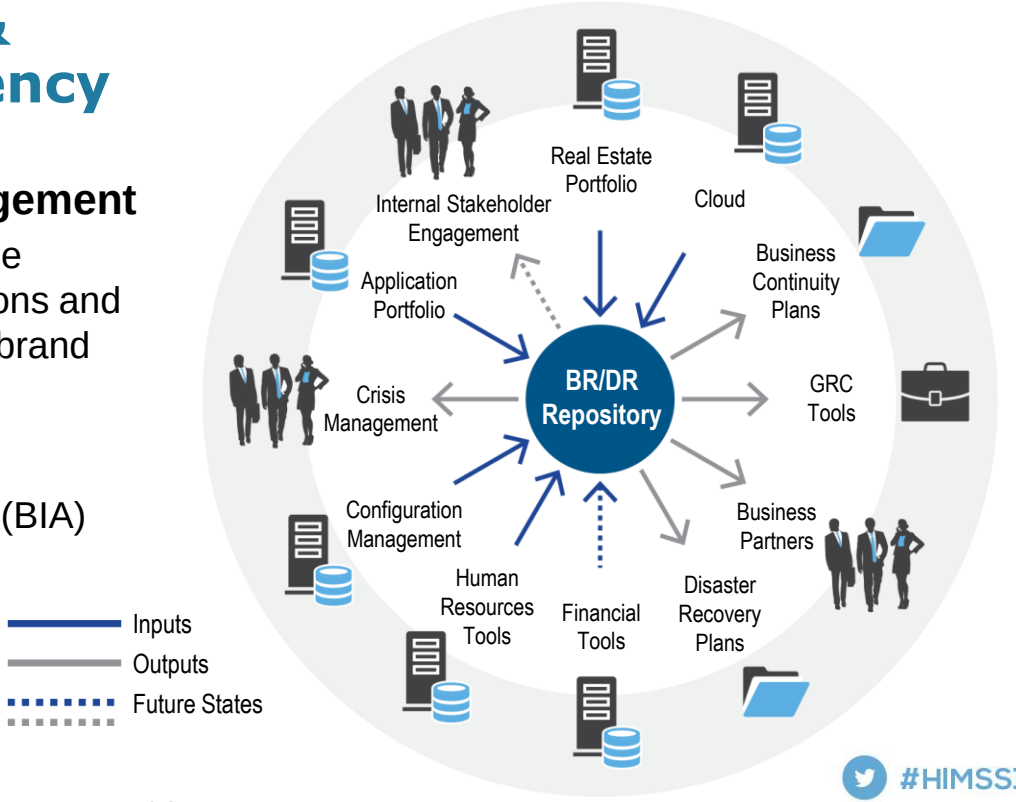




©HIMSS 2018

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



#HIMSS18
©HIMSS 2018

BEST-IN-CLASS CYBERSECURITY PROGRAM

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

Enterprise Security Architecture

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

#HIMSS18
©HIMSS 2018

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.

CAPABILITY DEVELOPMENT PROCESS

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

Training & Communication

Requirements

- Requirements Documents
  - Review architectural use cases, functional and non-functional requirements

Design

- Detailed Technical and Infrastructure Design Docs
- Test Plan & Cases
- Implementation Plan
- Procurement

Build

- Infrastructure provisioning
- DEV, TEST, PROD config / development

Test

- UAT, L&T, regression, system testing
- Operational runbooks
- Test Results Documented

Deploy

- Integration catalog updates
- Production cutover
- Complete Ops Handoff
  - Final reviews, signoff and warranty

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

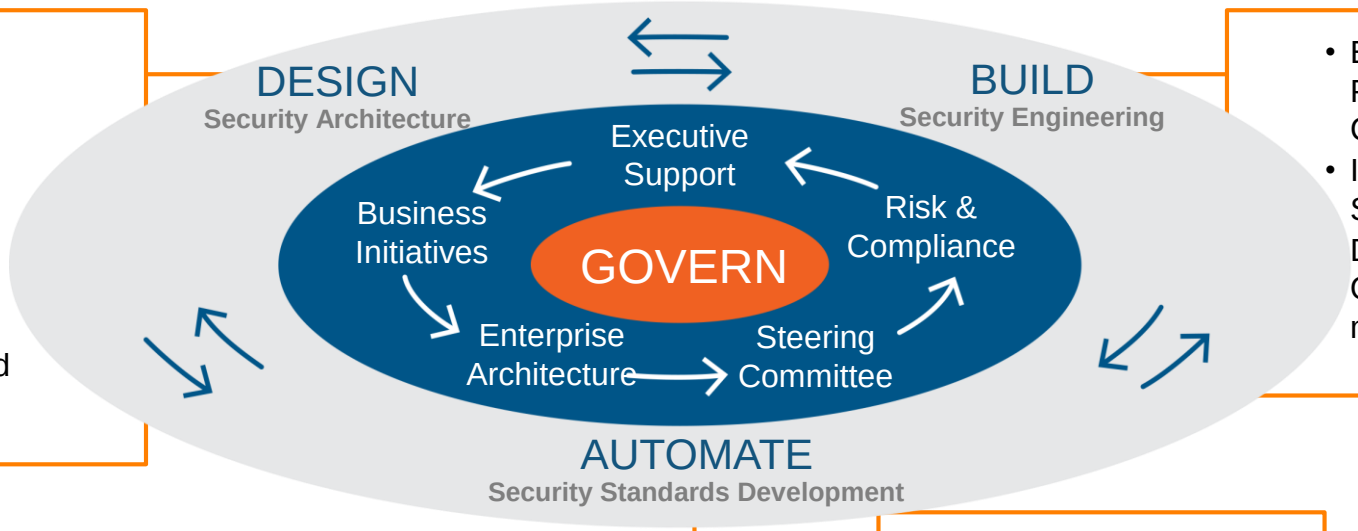
REGULATORY COMPLIANCE
Shifts in regulatory compliance and legislation

©HIMSS 2018

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.

- Enterprise Architecture / Business Alignment
- Security Architecture Strategy
- Design Principles and Conceptual Models



- Engineer Processes & Controls
- Integration Services
- Develop Operational models

- Standards Documentation
- Deliver Blueprints and Patterns
- Secure Build Kits

#HIMSS18
©HIMSS 2018

BEST-IN-CLASS CYBERSECURITY PROGRAM

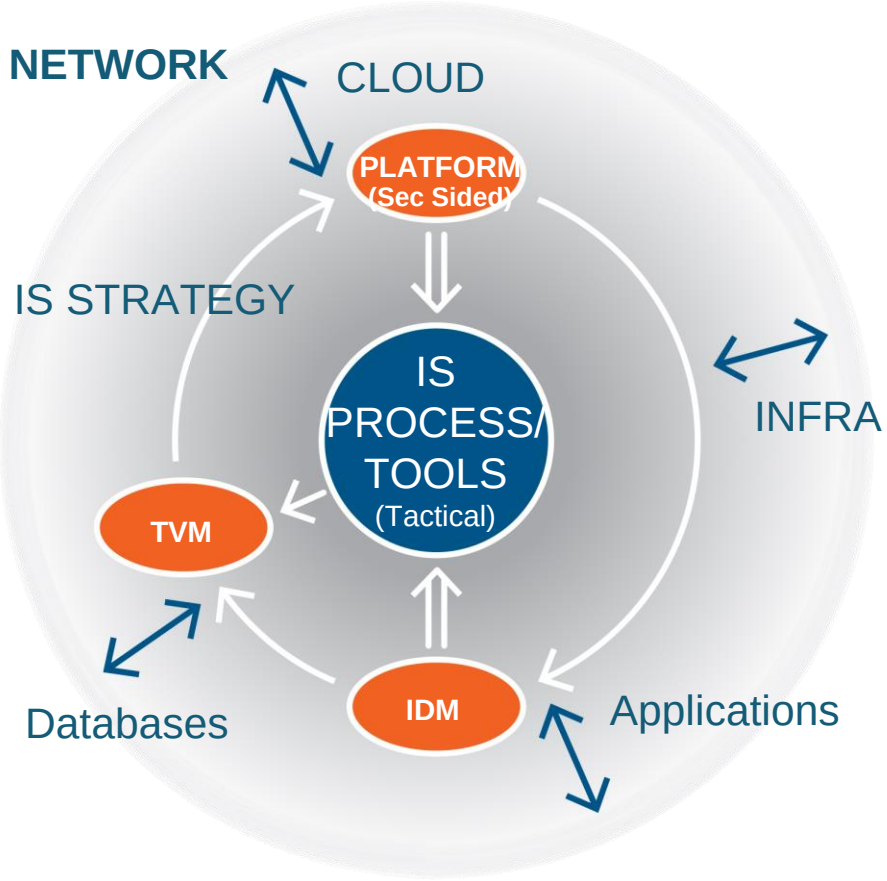
- Governance, Risk, and Compliance
- Security Architecture and Engineering
- Information Security Operations
- Cyber Defense Operations
- Business Engagement

Information Security Operations

- In-house, out-sourced, or hybrid approach
- Platform management
- Operational processes and standards enforcement
- Threat and vulnerability lifecycle management
- Operational metrics

©HIMSS 2018

Management and Metrics are influenced by all of these factors



©HIMSS 2018

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.

By Charlie Osborne for Zero Day | February 12, 2015 -- 12:54 GMT (04:54 PST) | Topic: Security

FierceHealthcare

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

by *Evan Sweeney* | Aug 9, 2017 1:33pm

HealthData Management All Sections

OCR hits Memorial Healthcare System with $5.5M fine

Business | Health | Local News

Premera negligent in data breach, 5 lawsuits claim

Originally published March 27, 2015 at 8:18 pm

#HIMSS18
©HIMSS 2018

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.

©HIMSS 2018

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.

©HIMSS 2018

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.

> 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

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

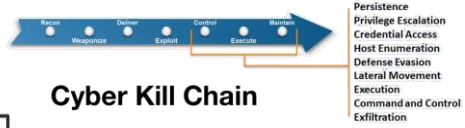
RESPOND

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

©HIMSS 2018

Cyber Defense & Investigation

Assume Breach Detection & Response Capabilities



Cyber Kill Chain

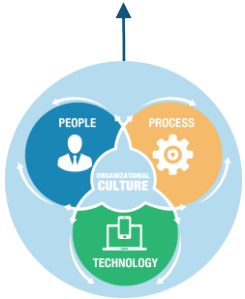
Advance Threat Analysis (ATA)
Proactive Threat Hunting

Threat Actors

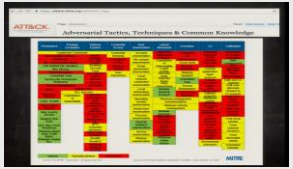
Adversary Cyber Attack

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)



TTP Defense Matrix

Threat Intelligence Platform

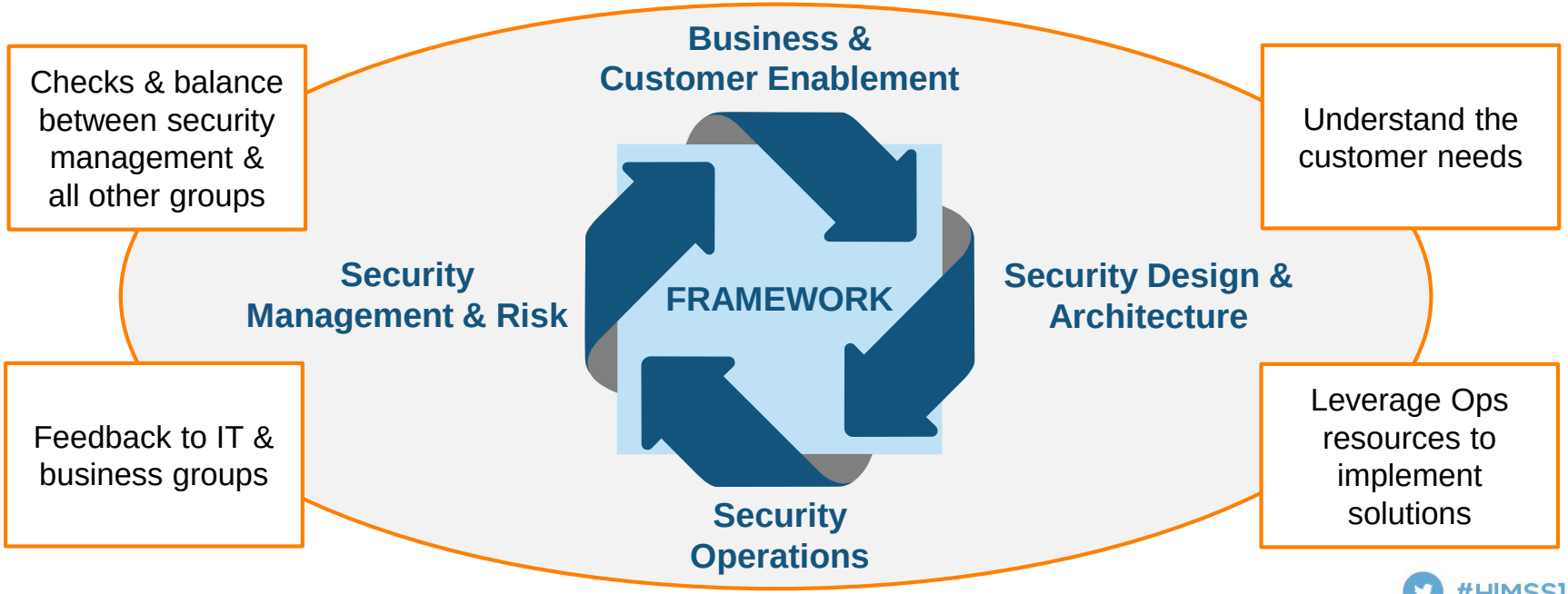
Security Big Data Lake

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



#HIMSS18
©HIMSS 2018

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

©HIMSS 2018

Roadmap to Building a Cybersecurity Program

Year 1

1. Create Strategic Plan
2. Cybersecurity Program Assessment
3. Create Prioritized Tactical Plan
4. Begin execution on people, process, & technology plan

Year 2

5. Continuous Improvement
6. Address the gaps
7. Validate appropriate talent mix

Year 3

8. Cybersecurity Program Maturity Assessment
9. Third Party Adversarial Test
10. Enhance strategic plan

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!

#HIMSS18
©HIMSS 2018

Appendix

©HIMSS 2018

Governance, Risk, and Compliance

Set forth the organization's security strategy and enable governance functions to manage security risk.

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

Security Architecture and Engineering

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

- Security Architecture
- Security Engineering
- Security Standards

Information Security Operations

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

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

Cyber Defense Operations

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

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

Business Engagement

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

- Business and IT Liaison
- IS Intake and Demand