Cybersecurity in a Digital Transformation World

Session 274, Feb. 14, 2019

KEVIN CHAREST
Divisional Senior Vice President and Chief Information Security Officer
Conflict of Interest

Kevin Charest, PhD

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

• Introduction and Background
• Understanding the Digital Transformation
• Evolving Threat Environment at Digital Speed
• Cybersecurity at Digital Speed
• Cybersecurity at the New Edge
• Cybersecurity When No One Can Be Trusted
• Cybersecurity Team Culture
• Closing
Learning Objectives

• Identify the digital threat environment and techniques for addressing new threat vectors

• Recognize processes for operating under increased standardization and automation

• Create and execute on strategies to control the flow of data in your organization

• Develop an appropriate workplace culture for employees to experiment
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

Operating Blue Cross and Blue Shield plans in FIVE states: IL, MT, NM, OK, TX

15 million members

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

Over 21,000 employees

208.3 million claims processed annually

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

1936 year founded

+$1 billion in IT spend

2,100 IT employees
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
Understanding the Digital Transformation

- Evolving Threat Environment at Digital Speed
- Cybersecurity at Digital Speed
- Cybersecurity at the New Edge
- Cybersecurity When No One Can Be Trusted
- Cybersecurity Team Culture
Evolving Threat Environment: Key Considerations

- From prevention to detection and response
- Assumed Compromise
- Threat Evolution
Evolving Threat Environment

DAILY NEWS

Hackers breach HealthCare.gov system, get data on 75,000

DAILY NEWS

Anthem's $16M breach settlement reminds others to assess their cyber risks

DAILY NEWS

Marriott announces data breach impacting 500 million hotel guests
Evolving Threat Environment at Digital Speed

Cybersecurity at Digital Speed

Cybersecurity at the New Edge

Cybersecurity When No One Can Be Trusted

Cybersecurity Team Culture
Cybersecurity at Digital Speed: Key Considerations

- **BUILD** MICROSERVICES AND APIs
  - Standardization
  - Disciplined processes
  - AUTOMATION
  - INCREASED SPEED

- CREATE A **SAFE AREA** FOR EMPLOYEES TO EXPERIMENT
Cybersecurity at Digital Speed:

Hackathons
Cybersecurity at Digital Speed

SECURITY AND PERFORMANCE REVIEWS

ADDING NEW CODE
Evolving Threat Environment at Digital Speed

Cybersecurity at Digital Speed

Cybersecurity at the New Edge

Cybersecurity When No One Can Be Trusted

Cybersecurity Team Culture
Cybersecurity at the New Edge: Key Considerations

Data is now everywhere
  • SaaS applications
  • BYOD
  • Unowned and uncontrolled
  • Cloud

Create and innovate on data control strategies

New perimeter is identity
Identity controls access
Cybersecurity at the New Edge: Data Control Strategies

Need for data classification in network

Data Stewards

Data Proliferations
Evolving Threat Environment at Digital Speed

Cybersecurity at Digital Speed

Cybersecurity at the New Edge

Cybersecurity When No One Can Be Trusted

Cybersecurity Team Culture
Cybersecurity When No One Can Be Trusted: Key Considerations

- Cloud Proliferation
- File Access Management
- Zero Trust Principle
Cybersecurity When No One Can Be Trusted: Zero Trust Environments

• 2017 Annual Cybercrime Report predicts cybercrimes cost world $6 trillion annually by 2021, up from $3 trillion in 2015

• 2017 Data Breach Study found that the global average cost of a data breach is $3.62 million.

• Stopping data breaches using zero trust is more effective than castle-and-moat process

• Asks who user is and how they accessed environment

• Trust but verify

• Technology: Multifactor authentication, IAM, orchestration, analytics, encryption, scoring and file system permissions.

• Policies: Give users least amount of access they need to accomplish a specific task
Evolving Threat Environment at Digital Speed
Cybersecurity at Digital Speed
Cybersecurity at the New Edge
Cybersecurity When No One Can Be Trusted
Cybersecurity Team Culture
Cybersecurity Team Culture: Key Considerations

- Shifting Team And Process Culture
- From Policy To Business Enablement
- Embedded In Projects
- Continuous Improvement
- Scientific Approach
Understanding the Digital Transformation

- Evolving Threat Environment at Digital Speed
- Cybersecurity at Digital Speed
- Cybersecurity at the New Edge
- Cybersecurity When No One Can Be Trusted
- Cybersecurity Team Culture
Questions

• Kevin Charest
  • Kevin_M_Charest@bcbsil.com
  • Kevin Charest, PhD

• Be sure to complete online session evaluation