HCSC
Health Care Service Corporation

Cybersecurity Overview

Ray Biondo
Divisional Senior Vice President
Chief Information Security Officer

Why Health Care Data?

- **Medicare Fraud:** Submit false claims from fictitious providers.
- **Medical Identity Theft:** Falsify IDs to seek medical care under the identity of another person.
- **Prescription Drugs:** Leverage legitimate prescription to obtain controlled substances for resale in illegal drug markets.
- **Black Market Exchange**: Sell records to other parties in exchange for anonymous digital currency.

Analysis of Data Breaches (2005-2015)

HCSC

Of 20 major global data breaches analyzed by HCSC…

35% involved infecting an endpoint with **malware**

85% involved the **lateral movement** of attackers from one machine to another

85% involved the compromise of an organization's **privileged users**

90% involved the compromise of an organization's **databases**

85% involved the compromise of an organization's **servers**

HCSC used a variety of sources to conduct this analysis.

The Number of Security Incidents Continues to Soar

HCSC

- The total number of security incidents detected by survey respondents climbed to **42.8 million** this year, an increase of 48% over 2013
- This is the equivalent of **117,339** incoming attacks ***per day, every day***

Source: PWC

High Growth in High-Profile Crimes

HCSC

While less frequent, incidents attributed to **nation-states**, **organized crime**, and **competitors** increased sharply in 2014

- **86%** jump in incidents by nation-states
- **64%** rise in compromises by competitors
- **26%** increase in incidents by organized crime

Source: PWC

Tactical Actions to Consider Immediately

HCSC

Four actions to consider in the short term to determine the current state of your environment and cybersecurity program:

1.  **Establish on-call incident response agreement(s) with forensic experts and outside counsel.**
2.  **Conduct a Breach Indicator Assessment and Threat Model to determine "Are you compromised and don't know it?"**
3.  **Perform a gap analysis and security risk assessment to determine your cybersecurity program's current maturity.**
4.  **Review your cybersecurity program strategy and incident readiness at the Board level.**

Source: PWC

Our Response to Current Cyber Threats

HCSC

Cyber Threat Tiger Team

- Cross-functional across Information Technology Group (ITG) areas
- Completed: Deep-dive forensics investigation on our systems, targeting cyber threats discovered at other health insurers
  - Team did not discover any significant evidence of the malware involved in recent attacks
- Continuing: Weekly meetings to discuss progress on breach protection work, as well as share up-to-date industry information about new threats

Our Response to Current Cyber Threats

HCSC

Mandiant Security Consulting Services

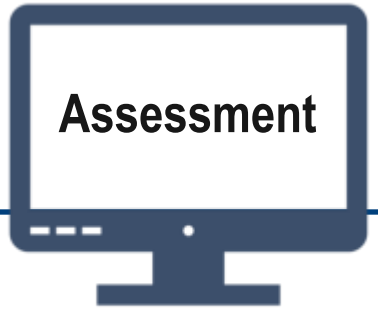
- Industry association recommendation
- Conducting a similar forensics investigation with proprietary tools and methods
- HCSC's Tiger Team forensics work was completed before engaging Mandiant

Current State of HCSC Information Security

HCSC

- User Campaign and Training
- Targeted Training for Privileged Users
- Formal Reporting and Response Channels

- Malware Protection
- Encryption of Data on mobile devices and in transit



- Internal Risk Assessment Service
- Internal and External Audits
- Compliance and Certifications (SOC1, SOC2, HITRUST)

Planned Improvements

HCSC

Security Awareness & Response

- Phishing Exercise and Training

Technical Initiatives

- Enhanced Malware Protection and Detection
- Encryption of Data at Rest and at the logical layer
- Enhanced Privileged User Management

Assessment

- Enhanced GRC solution (Governance, Risk, and Compliance)

HCSC
Health Care Service Corporation

Questions & Discussion