The Academy
The Health Management Academy

Quick-Hitting Survey

Cybersecurity Maturity

James Cheung, Associate, Research & Advisory
Melissa Stahl, Senior Manager, Research & Advisory

Executive Summary

Methodology

In March 2019, The Health Management Academy conducted a quick-hitting survey of Leading Health Systems to identify current cybersecurity maturity levels and assessment methods. The 9 responding Informatics Executives and Chief Information Officers (CIOs) represent health systems with an average Total Operating Revenue of $3.4 billion that own or operate 83 hospitals and have approximately 775,000 admissions per annum.

Key Findings

- On average, health systems scored 2.9 out of 5 overall on the NIST framework for cybersecurity maturity.
- Just over half (55%) of health systems utilize an additional maturity framework beyond NIST to assess cybersecurity maturity, most commonly HITRUST.
- Top cybersecurity priorities for health systems in 2019 include risk management and access management.

Results

The National Institute of Standards and Technology (NIST) framework is widely used to assess cybersecurity maturity in businesses and organizations. It is broken down into five categories: Identify, Protect, Detect, Respond, and Recover. Combined, they form the overall NIST score used to measure organizational cybersecurity maturity.

On average, the overall NIST score among responding health systems was 2.9 out of 5 (Figure 1). Of the five categories included in the NIST framework, executives reported to be most mature in Recover, with an average score of 3.2. This category refers to an organization's ability to restore systems in a timely manner following system impairment in a cybersecurity event.

The lowest scores were in the Identify and Detect categories, both averaging 2.7. The Identify category refers to an organization's ability to understand and manage cybersecurity risks to its systems while Detect refers to an organization's ability to identify and take action against the cybersecurity event itself.

Many health systems (55%) utilize an external vendor to assess their organization's cybersecurity maturity (Figure 2). Fewer health systems (22%) evaluate their cybersecurity maturity through internal assessments, while 22% utilize a combination of internal and external assessments. One executive reported using an external assessment every three years and internal assessments in between. There was no notable difference in the overall maturity scores between health systems that utilize internal versus external assessments.

FIGURE 1. NIST MATURITY AVERAGES

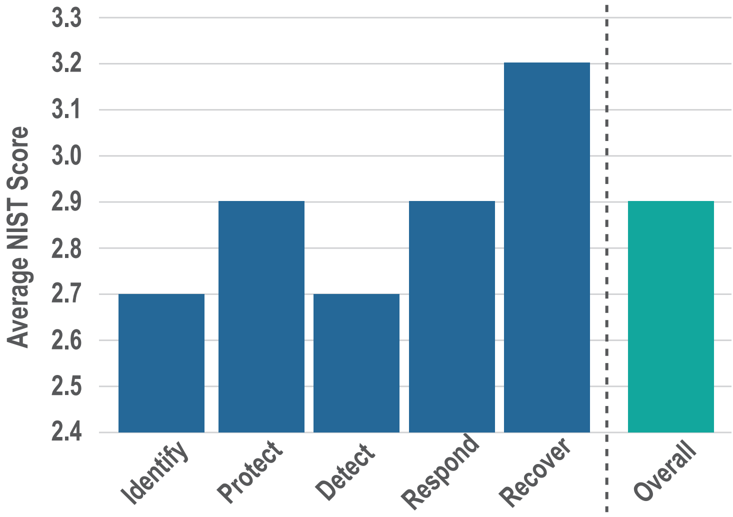
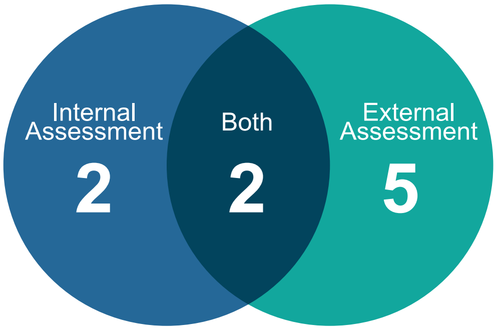


FIGURE 2. CYBERSECURITY NIST MATURITY ASSESSMENT METHOD



Health systems utilize a variety of external vendors to conduct cybersecurity maturity assessments (Figure 3). While some health systems report utilizing multiple external vendors to conduct these assessments, the only vendor that was used by more than one health system respondent was Cynergistek.

In order to obtain a comprehensive picture of the organization’s cybersecurity maturity, just over half (55%) of health systems utilize additional maturity frameworks beyond NIST. The most common additional framework utilized is HITRUST, followed by the COBIT Maturity Model, Cisco Cybersecurity Maturity Framework, and the Center for Internet Security (CIS) Top 20 Critical Security Controls (Figure 4). However, there was no significant difference in overall maturity scores between health systems that utilize only the NIST framework and those that utilize additional frameworks.

Reflective of health systems’ current maturity levels, many organizations are prioritizing functions that support the Identify and Detect categories in the NIST framework. In particular, risk management and access management are the two most common cybersecurity priorities for 2019 (Figure 5).

FIGURE 3. EXTERNAL CYBERSECURITY ASSESSMENT VENDORS

- Cynergistek
- RSM
- Protiviti
- Sirius
- Security Risk Advisors
- Meditology
- Deloitte
- Roundtower
- Fortified Health
- Neopahsi

FIGURE 4. ADDITIONAL CYBERSECURITY MATURITY FRAMEWORKS

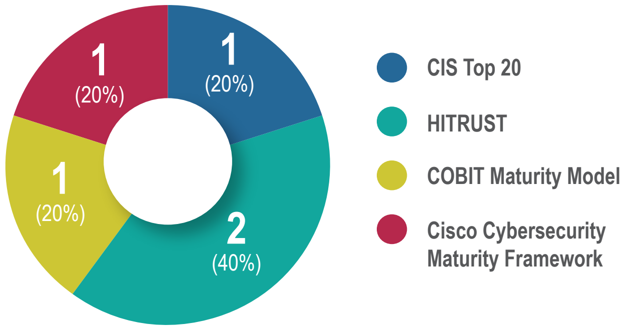
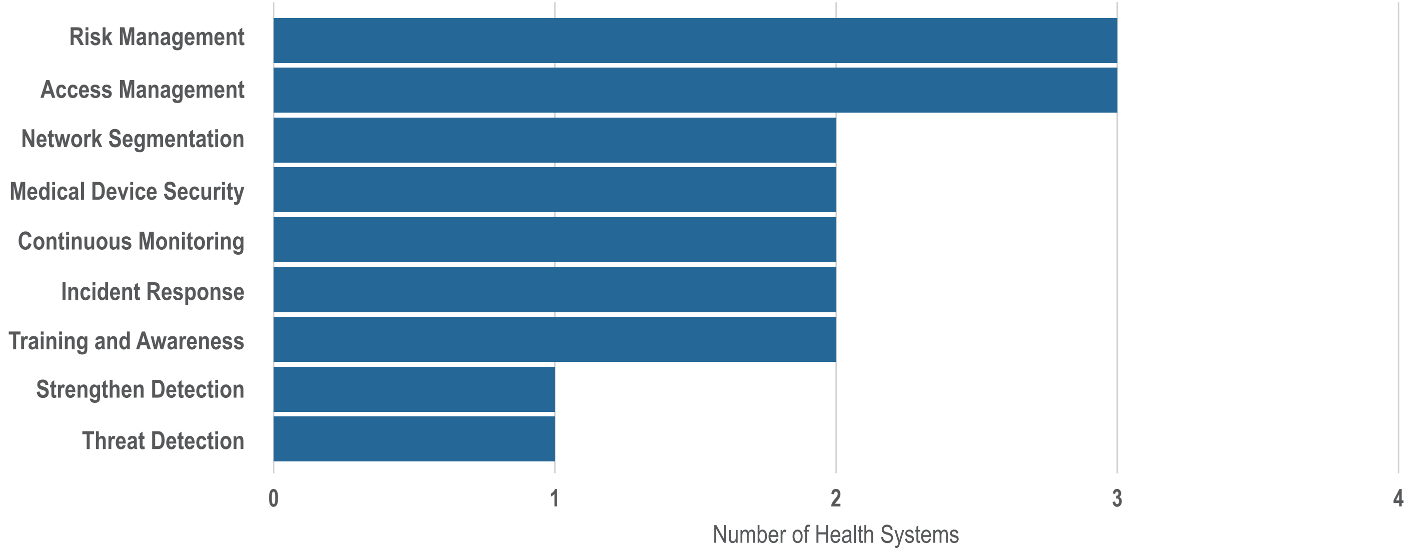


FIGURE 5. 2019 CYBERSECURITY PRIORITIES


Risk Management
Access Management
Network Segmentation
Medical Device Security
Continuous Monitoring
Incident Response
Training and Awareness
Strengthen Detection
Threat Detection
Number of Health Systems