Cybersecurity Survey Results

4 November 2015

Learning Objectives

- Identify the tools in use to secure the healthcare environment.
- Learn how organizations assess, prevent and detect cybersecurity events.
- Learn which threat motivators respondents were most concerned about.
- Determine which items are the biggest barriers to mitigate cyber security incidents.

History of HIMSS Security Research

- First survey conducted in 2008 in USA
  - Three-quarters of respondents conducted risk analysis
  - Spent less than three percent of IT budget on security
  - User-based and role-based controls to secure patient information
- Conducted for the sixth time in 2014 in USA
  - Greatest “security threat motivator” encountered in healthcare is healthcare workers snooping into records
  - 92 percent conducted in risk analysis
  - Half reported spending three percent or less of their overall IT budget on securing patient data

HIMSS Latin America
CYBERSECURITY SURVEY 2015

SUMMARY RESULTS

CYBERSECURITY SURVEY 2015

Motives for Improving Information Security Posture

Top motivators for improving information security environments included **results of risk assessment** and **virus/malware and vulnerability analysis results**

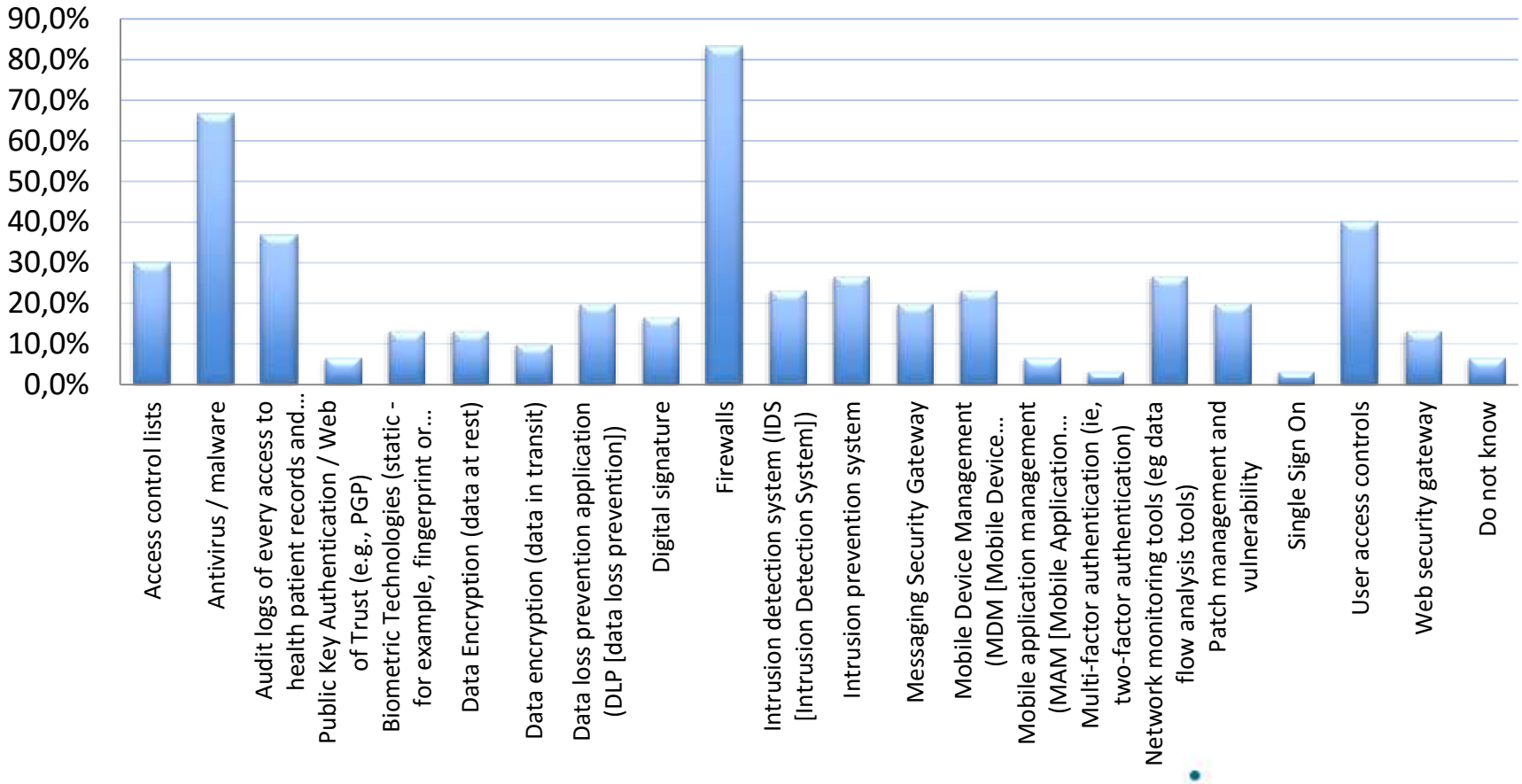
Information Security as Business Priority

of respondents indicated **information security** had increased as a **business priority**

Enhanced Information Security Capabilities

- 73% Improved Continuity of IT
- 67% Network Security
- 63% Data Loss Prevention
- 33% Disaster Recovery
- 27% Improving the Protection of Endpoints

Information Security Tools in Place

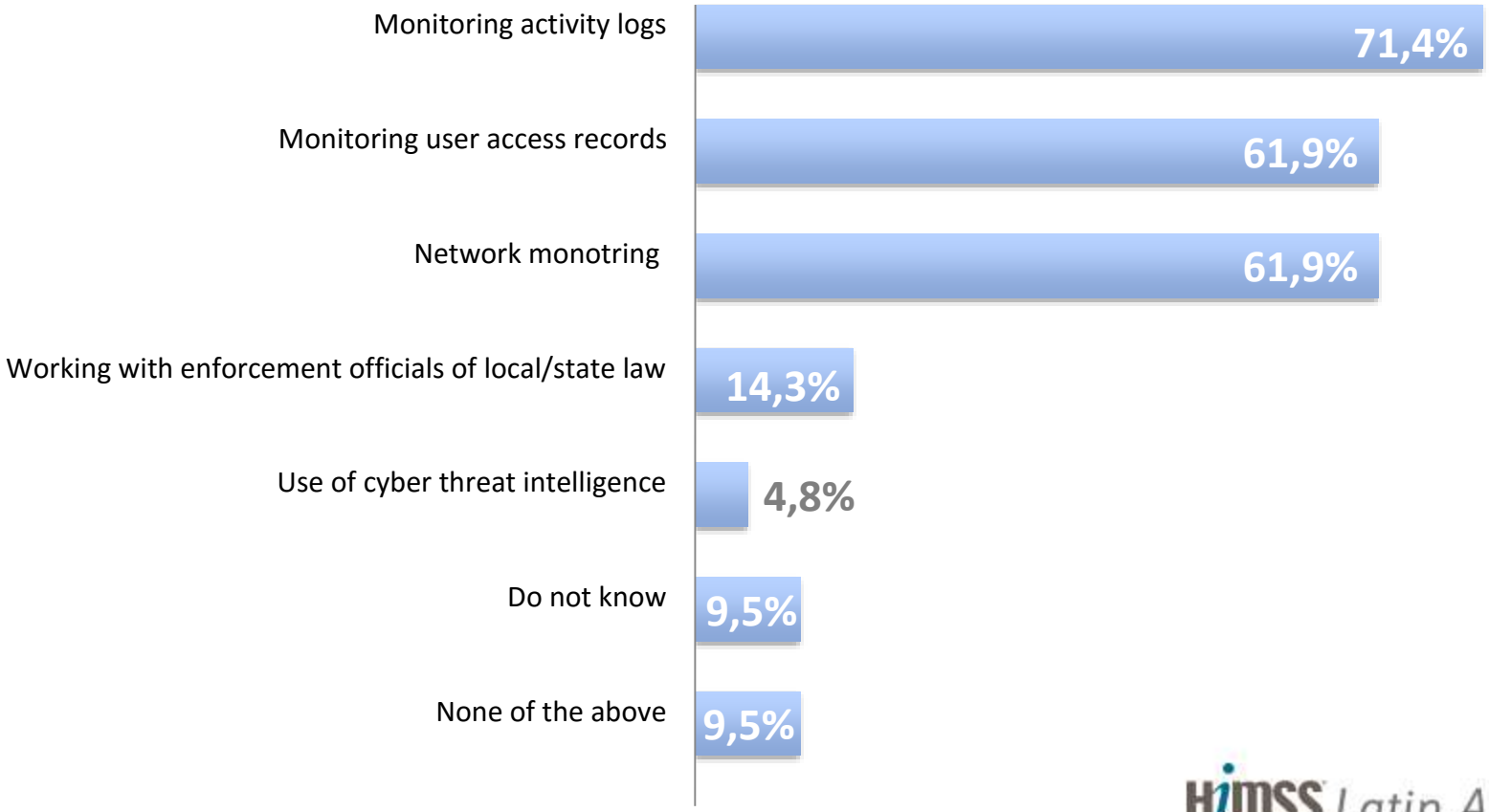


Ability to Protect Information

Rate the options on a scale 1-7, where one is "not prepared" and seven is "fully prepared"

- Brute Force Attacks (4.75)
- Exploit Known Vulnerabilities (4.6)
- Phishing Attacks (4.5)
- Negligent Insider Attacks (4.4)
- Malicious Insider Activity (4.4)
- Zero Day Attack (4.3)
- Attacks Denial of Service (DoS) (4.2)
- Advanced Persistent Threat of Attacks (4.1)

Techniques Used to Detect and Investigate Incidents



Preparedness to Detect Security Incidents

Rate the options on a scale 1-7, where one is "not prepared" and seven is "fully prepared"

Statement	Average
Brute Force Attack	4.25
Exploitation of Known Software Vulnerabilities	4.25
Malicious insider attacks	4.20
Negligent insider attacks	4.15
Zero Day Attacks	4.05
Phishing Attacks	4.00
Denial of Services (DoS)/Distributed Denial of Services (DDoS)	4.00
Advanced Persistent Threat (APT) Attacks	3.90

Consequences of Security Incidents

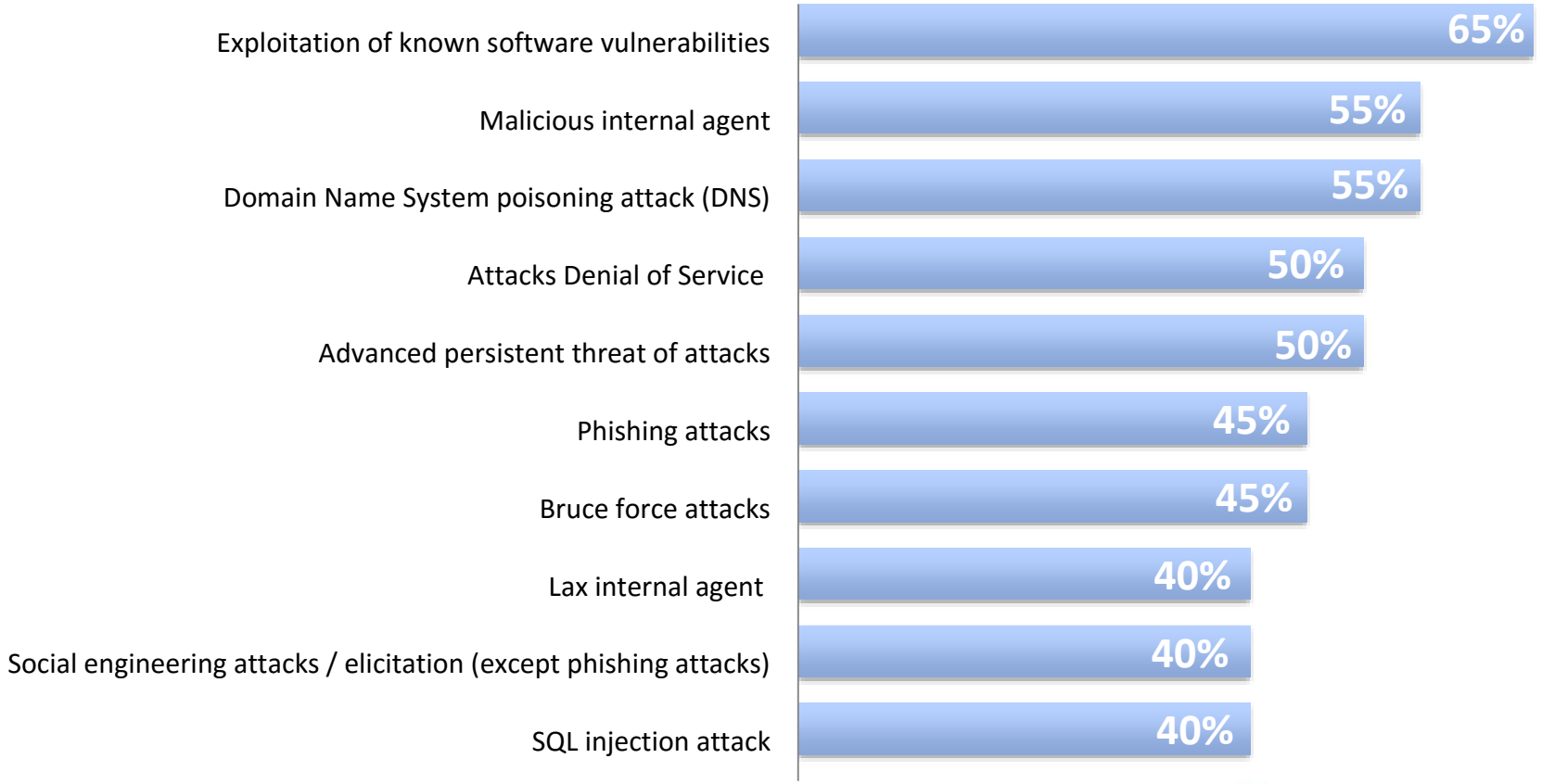
- 31% Loss of Data/Information
- 19% Limited Disruption to Operations
- 19% Significant Impact on IT Systems
- 6% Damage to IT Systems
- 6% Other Impact

Exploitation of known software vulnerabilities is a concern

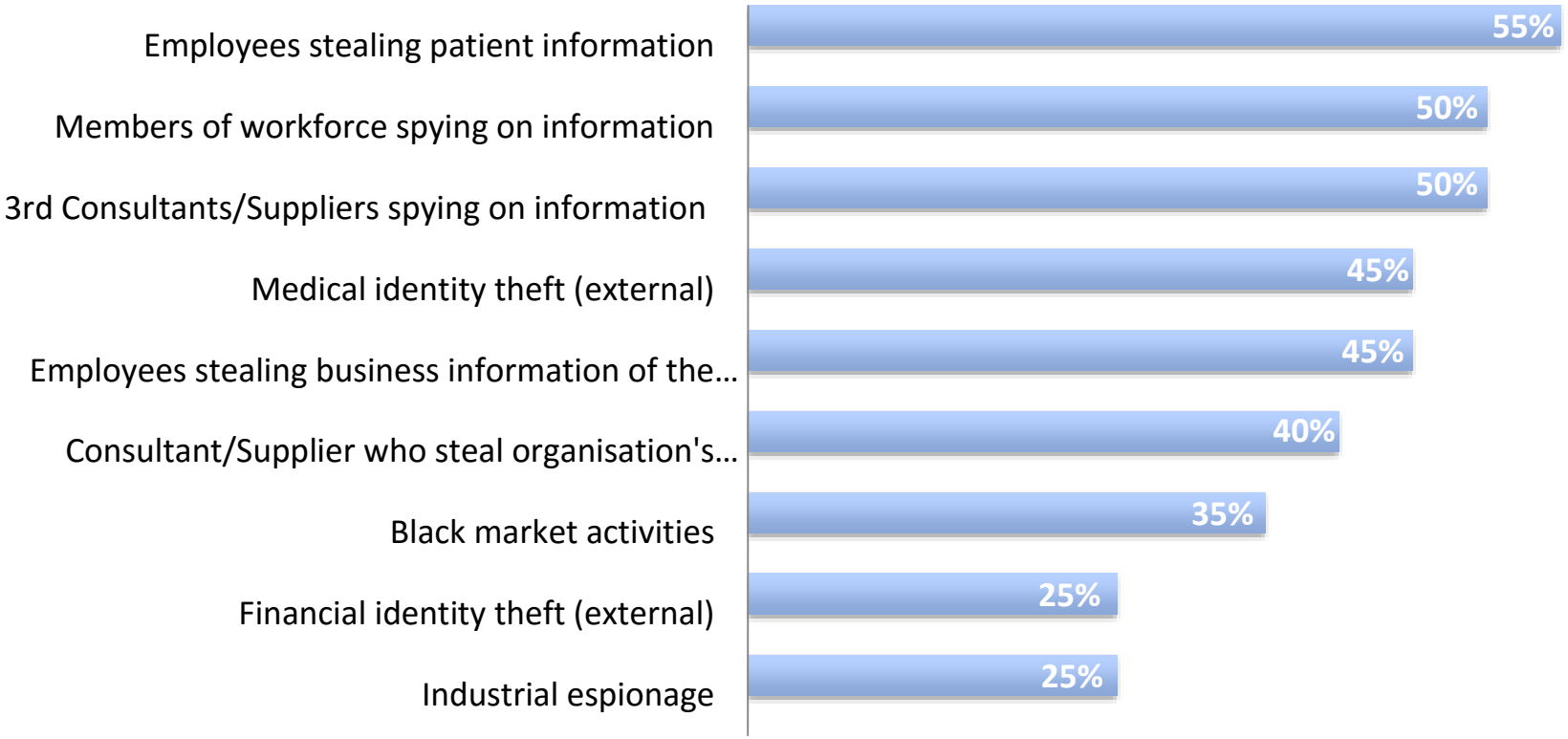
Respondents are **highly concerned** about exploitation of **known software vulnerabilities** in the future

65% polled named it as their biggest concern.

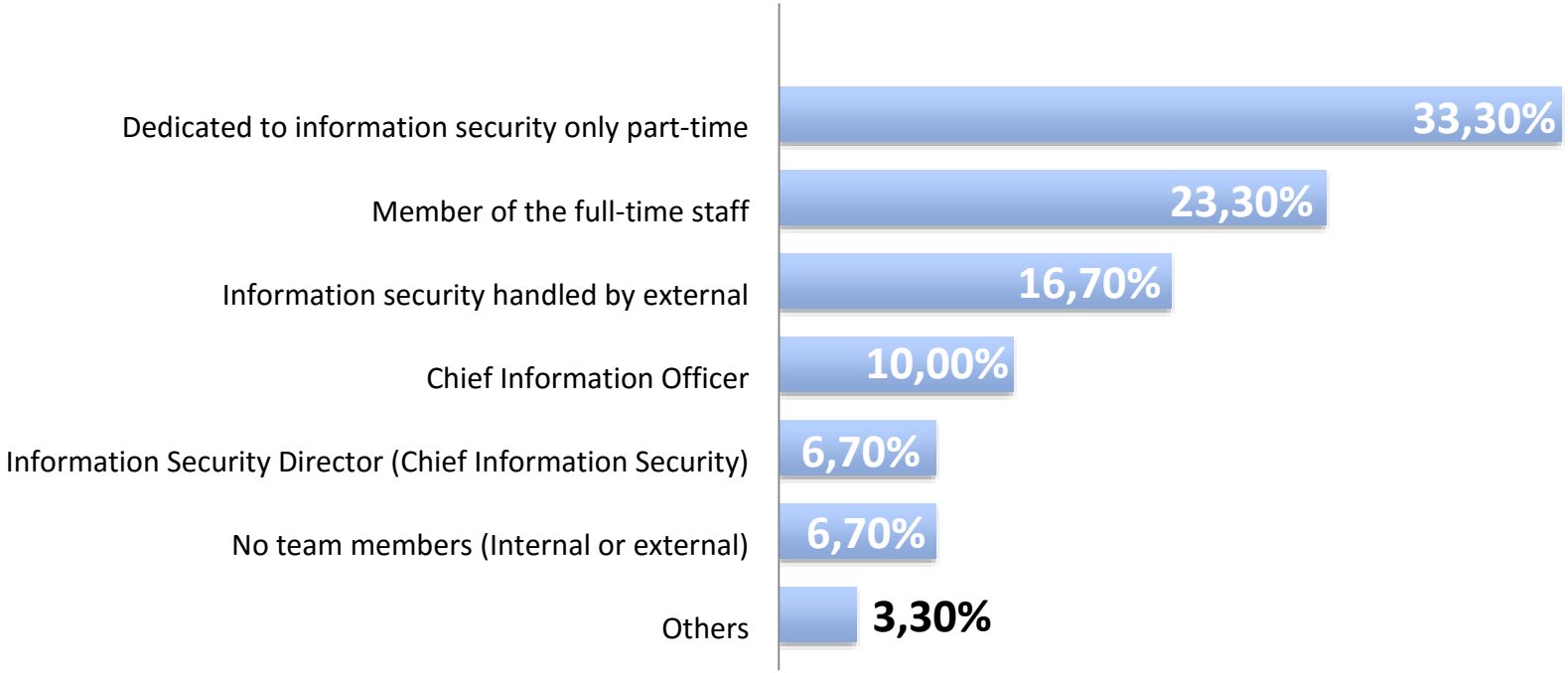
Significant Threats of the Future
Top Ten



Drivers of the Most Common Threats



Staff Allocation to Information Security Function



Barriers to Information Security

Count	Percent
Lack of adequate cybersecurity staff	60%
Lack of financial resources	55%
Too many emerging threats	25%
Lack of know-how to use and effective implementation	20%
Lack technologies and tools for effective use	20%
Too many endpoints	20%
Too many users too much for provisioning and deprovisioning of accounts in a timely and effective	20%

Conclusions

- Survey respondents' organizations are challenged with respect to resources:
  - Staffing
  - Processes
  - Tools
- Software vulnerabilities and Insider threat are of great concern
- Level of uncertainty still surrounds ability to protect against current and future attacks (internal and external)

Questions

Lisa A Gallagher, BSEE, CISM, CPHIMS, FHIMSS

VP, Technology Solutions

HIMSS North America

lgallagher@himss.org