DIGITAL GUARDIAN®

FORRESTER®

Addressing the Top 5 Healthcare IT Security Risks

Chris Sherman, Analyst, Forrester Research

Brian Mullins, VP of Product Marketing, Digital Guardian

Agenda

- Top 5 IT Trends Putting Healthcare Providers At Risk
- Top 5 Security Challenges Experienced By Providers
- Healthcare Security Budget Trends
- Forrester Recommendations
- 6 Reasons to Consider Digital Guardian
- Q & A

About Chris Sherman

- Analyst, Forrester Research
- Has covered endpoint security and data privacy for 5 years
- Previously worked as a Research Associate at Mass General Hospital

About Brian Mullins

- VP, Content & Product Marketing
- 20 years in B2B Marketing
- 6 years in Security Marketing
- Came to DG from Imprivata
- Patent holder – Electronic Notepad

DIGITAL GUARDIAN®

FORRESTER®

Addressing the Top 5 IT Security Risks – A Survey of Healthcare Security Pros

Webinar

Chris Sherman

Agenda

- *Research Overview*
- *Top 5 IT Trends Putting Healthcare Providers At Risk*
- *Top 5 Security Challenges Experienced By Providers*
- *Healthcare Security Budget Trends*
- *The Path Forward*

Agenda

- *Research Overview*
- *Top 5 IT Trends Putting Healthcare Providers At Risk*
- *Top 5 Security Challenges Experienced By Providers*
- *Healthcare Security Budget Trends*
- *The Path Forward*

Putting The Spotlight On Healthcare Providers

Research methodology:

- Surveyed 69 healthcare providers
- Evaluated 62 past Forrester healthcare client inquiries
- Interviewed 45 healthcare provider security professionals
- Interviewed 16 healthcare security consultancies and vendors

Putting The Spotlight On Healthcare Providers (con't)

We surveyed healthcare security decision makers on a number of topics:

- Social Media
- Priorities
- General Security Topics
- Emerging Technology Risk & Policy
- Sourcing Strategy
- Organizational Structure
- Governance, Risk & Compliance
- Breaches
- Application Security
- Network Security & Security Operations
- Identity & Access Management
- Mobile Security
- Data Security
- Content Security
- Client Security
- Risk Attitudes
- Security Services
- Security Budgets & Spending
- VSB Budget
- Security & Privacy
- Customer-Facing Security

Agenda

- *Research Overview*
- *Top 5 IT Trends Putting Healthcare Providers At Risk*
- *Top 5 Security Challenges Experienced By Providers*
- *Healthcare Security Budget Trends*
- *The Path Forward*

IT Trends Affecting Healthcare Security Practices

Healthcare S&R Pros were asked to rate their level of concern with 16 IT trends:

1. *Infrastructure-as-a-service*
2. *Platform-as-a-service*
3. *Software-as-a-service solutions*
4. *Virtualization in the data center*
5. *Desktop/ Application virtualization*
6. *Consumer-oriented communication and file-sharing tools run on non-corporate resources*
7. *Employee-provisioned applications*
8. *Employee-provisioned devices for business use*
9. *IT and business process offshoring or outsourcing*
10. *The business' need for innovation*
11. *Greater IT connectivity, collaboration, and information with business partners*
12. *Machine-to-machine or "Internet of things" solutions*
13. *Big data analytics for business decision-making*
14. *Software defined networking*
15. *Deployment of real-time communications over IP*
16. *Bring your own device initiatives*

Top Five Security Risk Exposures In Healthcare

US Healthcare Security Risks About Which S&R Pros Are "Very Concerned"

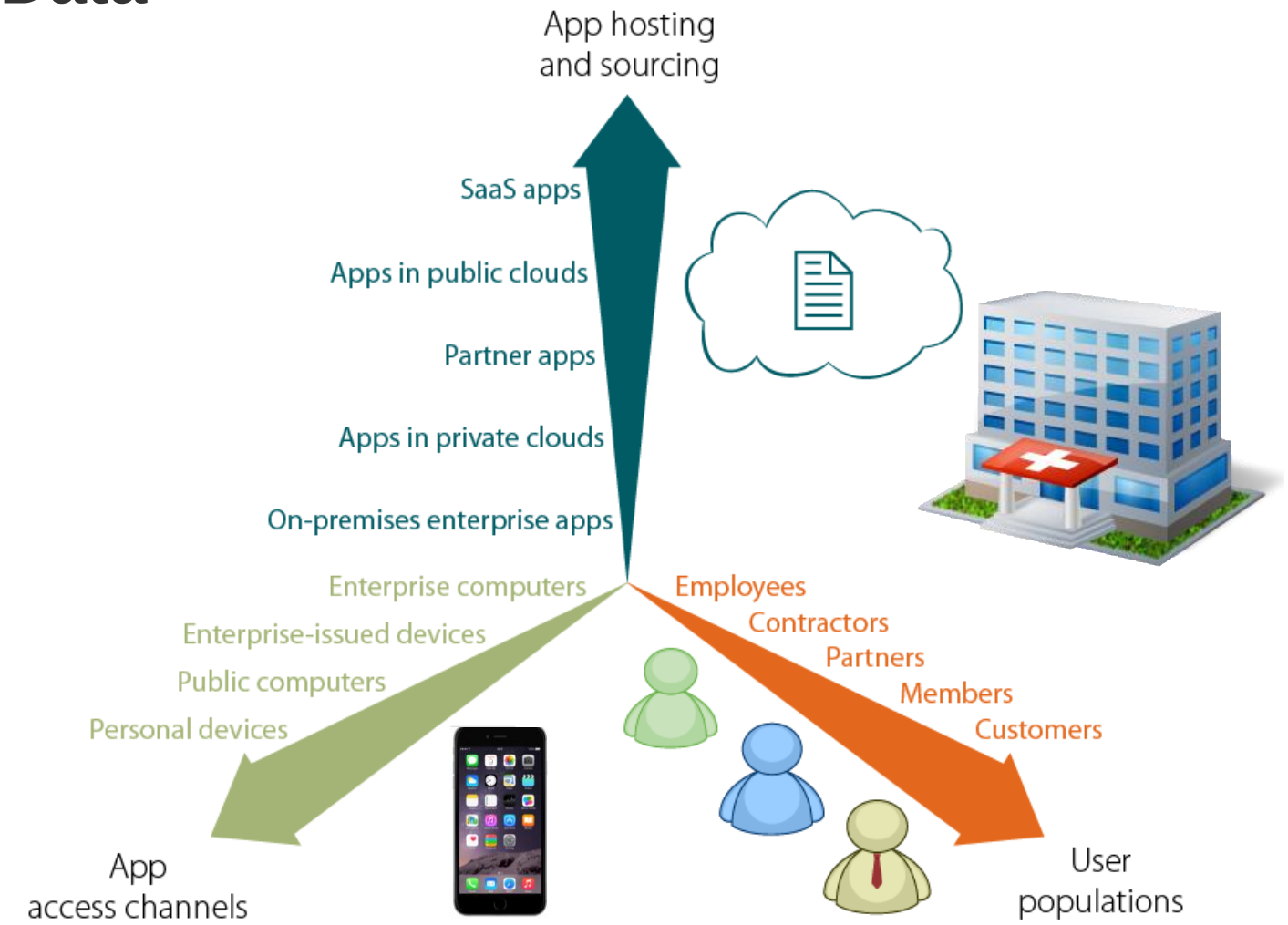
(5 on a scale from 1 [not at all concerned] to 5 [very concerned])

26%	Consumer-oriented communication and file-sharing tools run on noncorporate resources
20%	Employee-provisioned applications (including software and web services like Facebook and Twitter)
20%	Software-as-a-service solutions
19%	Bring-your-own-device initiatives
17%	Employee-provisioned devices for business use

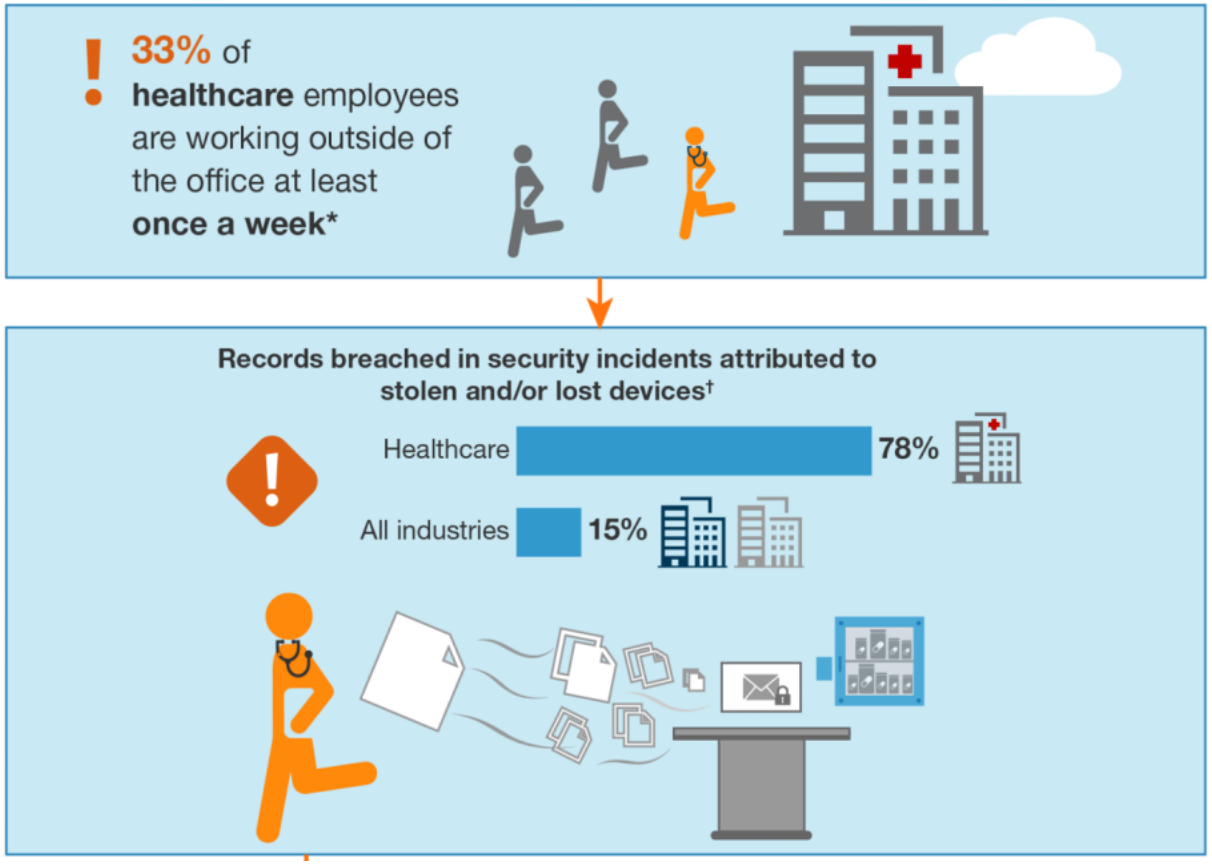
Base: 69 US healthcare security decision-makers

Source: Forrester's Global Business Technographics® Security Survey, 2015

Most Of The Top Concerns Are Rooted In The Lack Of Control Over Health Data

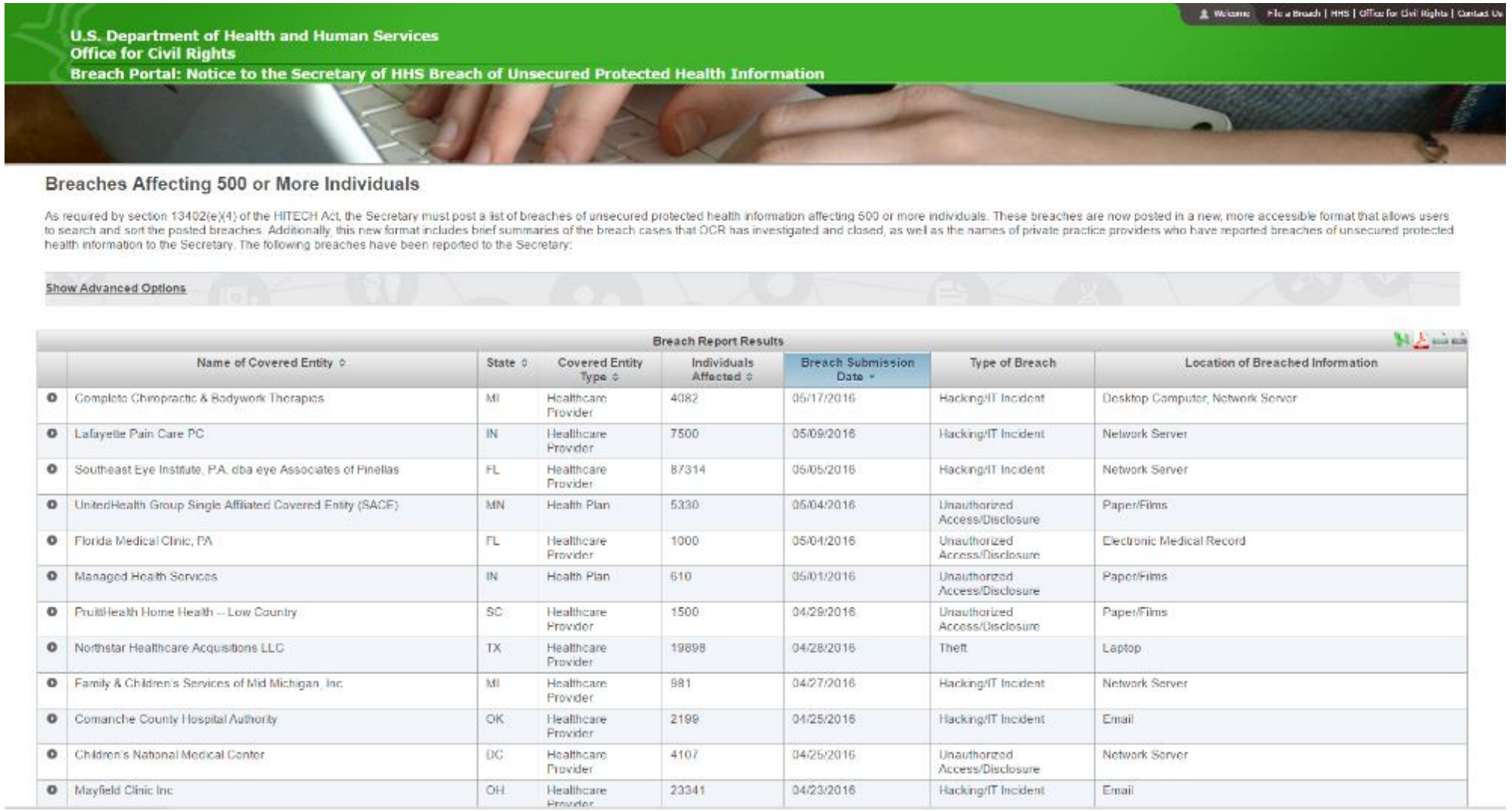


Healthcare Orgs Have Cause To Worry About Employee Devices



*Base: 521 global information workers in the healthcare provider industry
†Note: From 2005 to 2014, all industries had a total of 2,431 security incidents and 303,836,429 total number of records compromised; in that time, the healthcare industry had a total 795 total security incidents and 45,516,052 total number of records compromised.

HIPAA Fines And Audits Are Upon Us



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Complete Chiropractic & Bodywork Therapies	MI	Healthcare Provider	4082	05/17/2016	Hacking/IT Incident	Desktop Computer, Network Server
Lafayette Pain Care PC	IN	Healthcare Provider	7500	05/09/2016	Hacking/IT Incident	Network Server
Southeast Eye Institute, P.A. dba eye Associates of Pinellas	FL	Healthcare Provider	87314	05/05/2016	Hacking/IT Incident	Network Server
UnitedHealth Group Single Affiliated Covered Entity (SACE)	MN	Health Plan	5330	05/04/2016	Unauthorized Access/Disclosure	Paper/Films
Florida Medical Clinic, PA	FL	Healthcare Provider	1000	05/04/2016	Unauthorized Access/Disclosure	Electronic Medical Record
Managed Health Services	IN	Health Plan	610	05/01/2016	Unauthorized Access/Disclosure	Paper/Films
PruittHealth Home Health -- Low Country	SC	Healthcare Provider	1500	04/29/2016	Unauthorized Access/Disclosure	Paper/Films
Northstar Healthcare Acquisitions LLC	TX	Healthcare Provider	19898	04/28/2016	Theft	Laptop
Family & Children's Services of Mid Michigan, Inc	MI	Healthcare Provider	981	04/27/2016	Hacking/IT Incident	Network Server
Comanche County Hospital Authority	OK	Healthcare Provider	2199	04/25/2016	Hacking/IT Incident	Email
Children's National Medical Center	DC	Healthcare Provider	4107	04/25/2016	Unauthorized Access/Disclosure	Network Server
Mayfield Clinic Inc	OH	Healthcare Provider	23341	04/23/2016	Hacking/IT Incident	Email

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Agenda

- *Research Overview*
- *Top 5 IT Trends Putting Healthcare Providers At Risk*
- *Top 5 Security Challenges Experienced By Providers*
- *Healthcare Security Budget Trends*
- *The Path Forward*

Security Challenges Faced By Healthcare S&R Pros

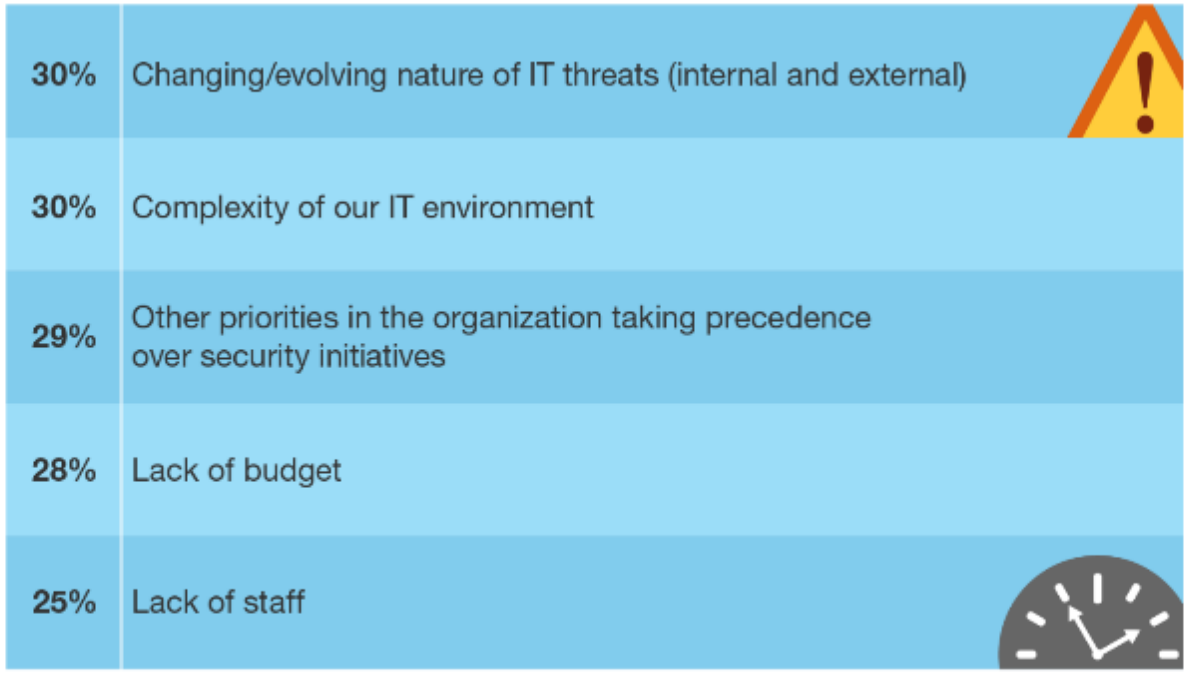
Participants were asked to rate their difficulty in addressing each of the following challenges:

1. *Lack of budget*
2. *Lack of staff (the security team is understaffed)*
3. *Lack of visibility and influence within the organization (including difficulty making business cases)*
4. *Unavailability of products/services that fit our needs*
5. *Unavailability of security employees with the right skills*
6. *Complexity of our IT environment*
7. *Changing/evolving nature of IT threats (internal and external)*
8. *Day-to-day tactical activities taking up too much time*
9. *Other priorities in the organization taking precedence over security initiatives*
10. *Inability to measure the effectiveness of our security program*
11. *Too many security vendors to manage*

Top Five Security Challenges In Healthcare

US Healthcare Security “Critical” Priorities

(5 on a scale from 1 [not a challenge] to 5 [major challenge])



Base: 69 US healthcare security decision-makers

Source: Forrester’s Global Business Technographics® Security Survey, 2015

Healthcare Endpoints Present A Unique Set Of Risks

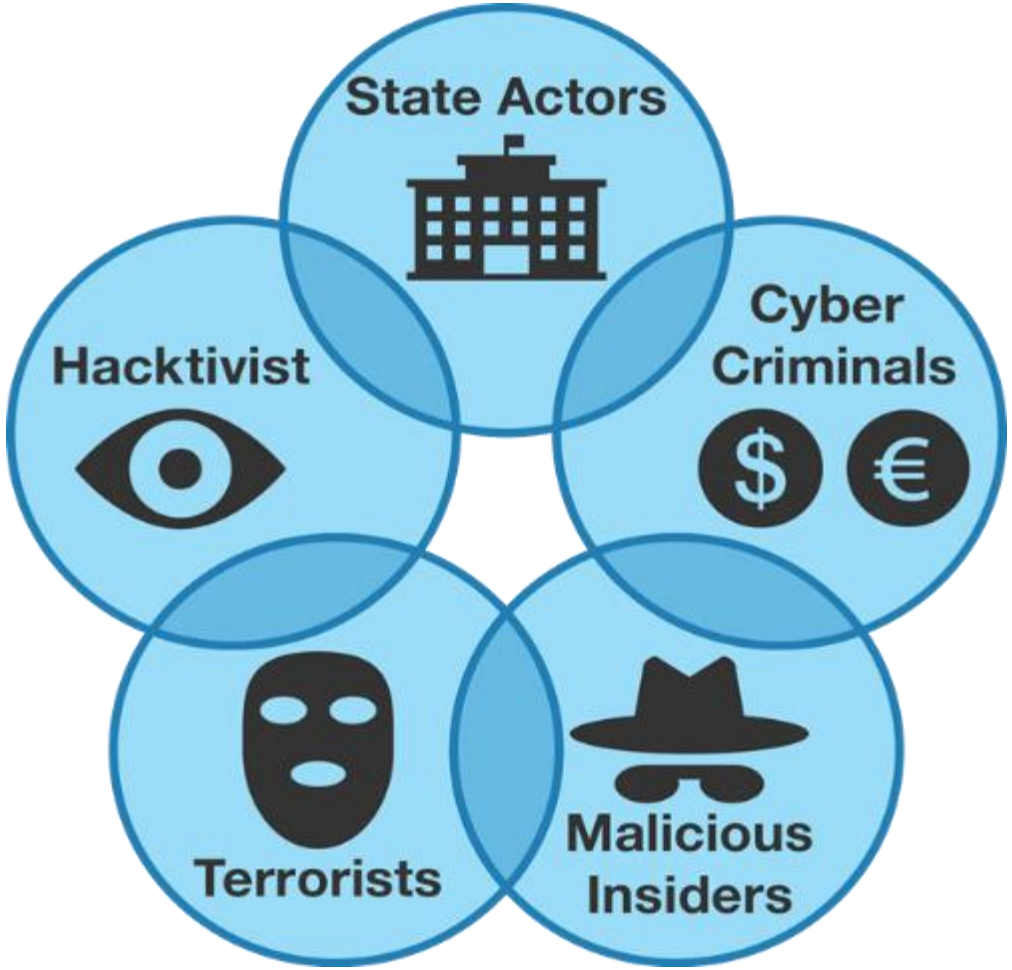
Denial-of-Service

Therapy Manipulation

Patient Data Theft

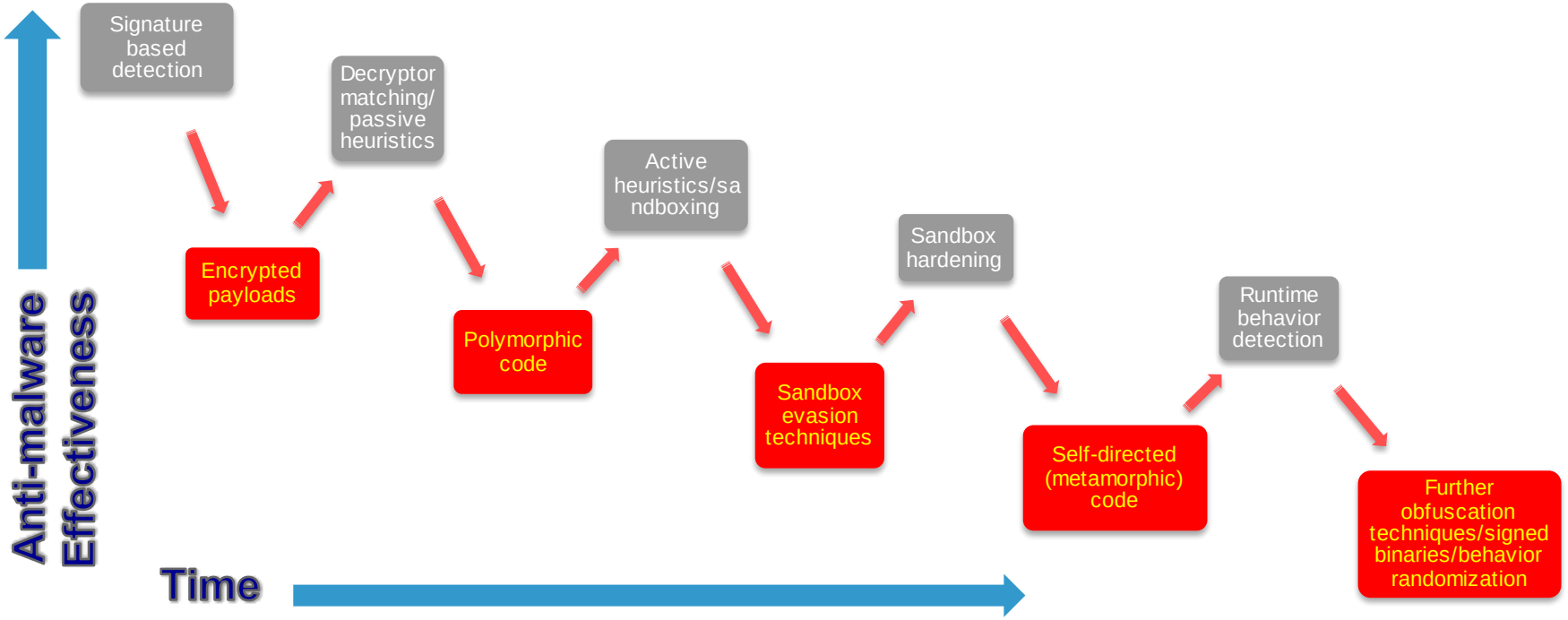
Asset Damage

Healthcare Security Pros Are Up Against Five Major Threat Actors



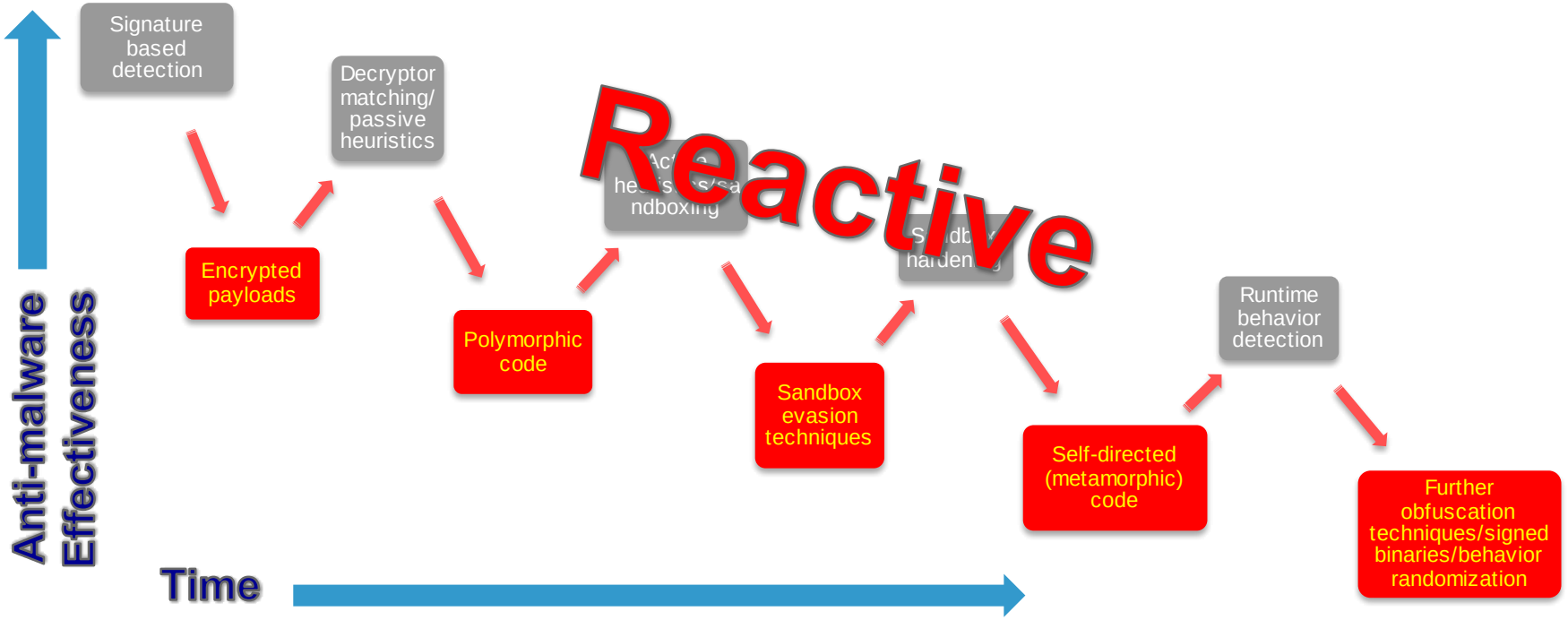
Defenders Face An Ongoing Anti-Malware Technology Arms Race

25% of all reported data breaches involve malware

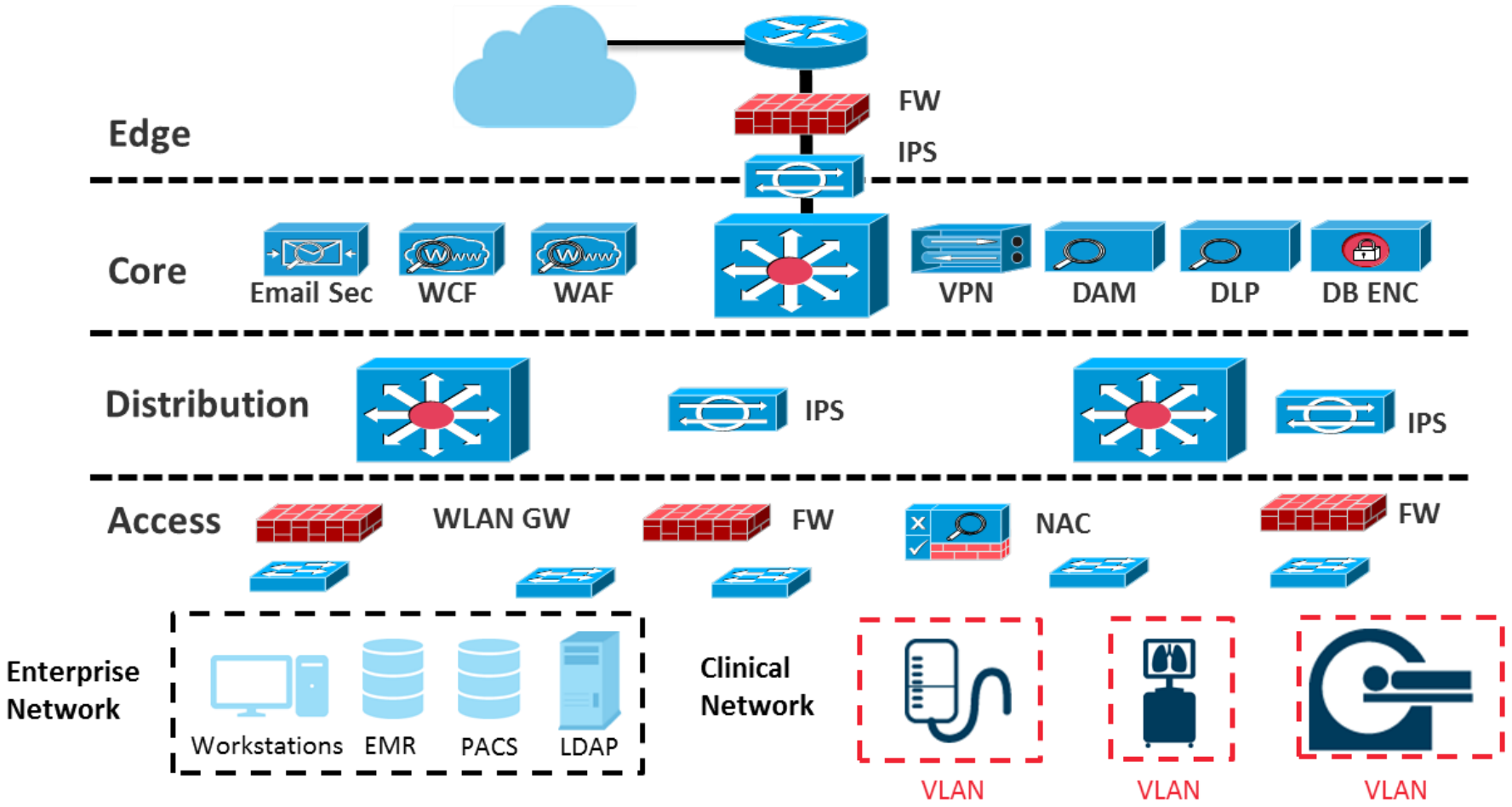


Defenders Face An Ongoing Anti-Malware Technology Arms Race

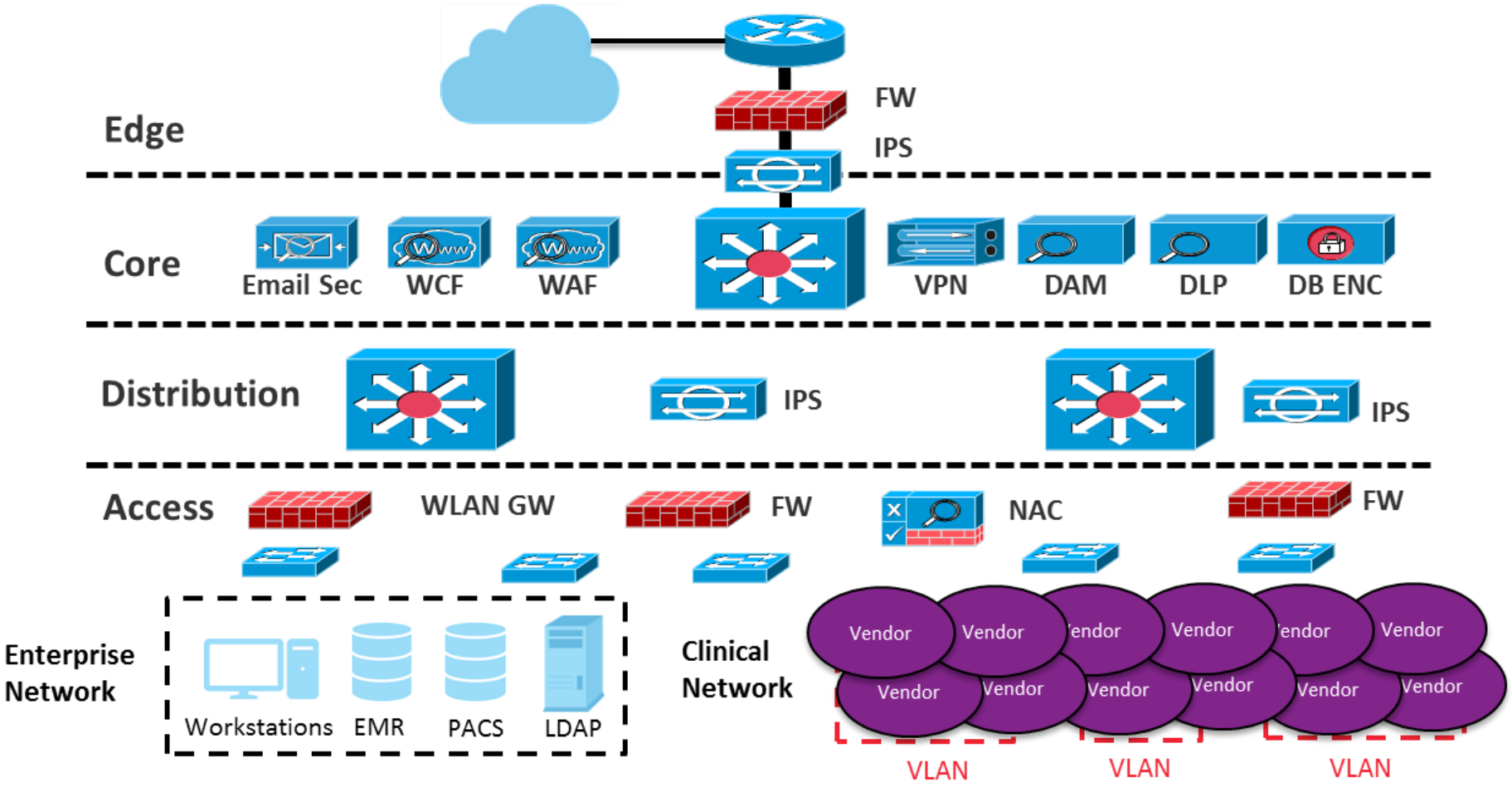
25% of all reported data breaches involve malware



Flat Hospital Networks Present Opportunities For Attackers



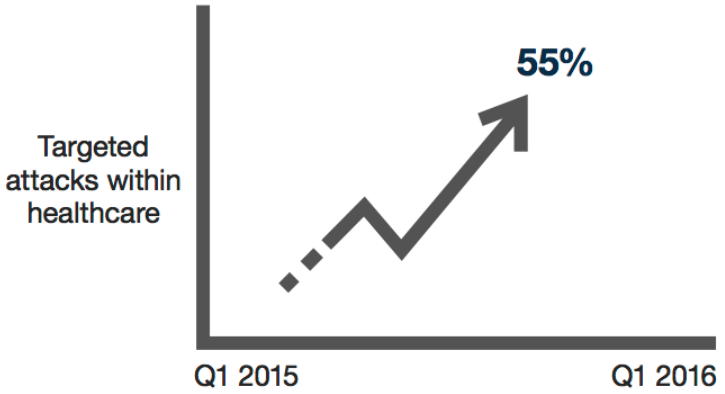
Complexity Is The Primary Enemy



Hospitals Are Especially Concerned With Targeted Attacks

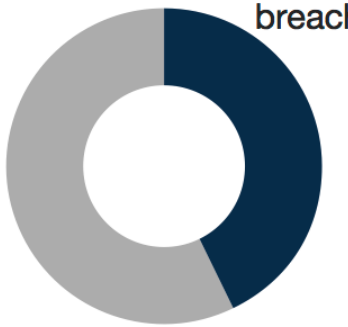
59 targeted attacks against healthcare orgs led to public breaches in 2016

55% increase in targeted attacks within healthcare from 2015 to 2016 (Cyberfactors)



2,580,988 healthcare records were lost in 2016 (Cyberfactors):

43% of all healthcare orgs experienced a breach in 2016



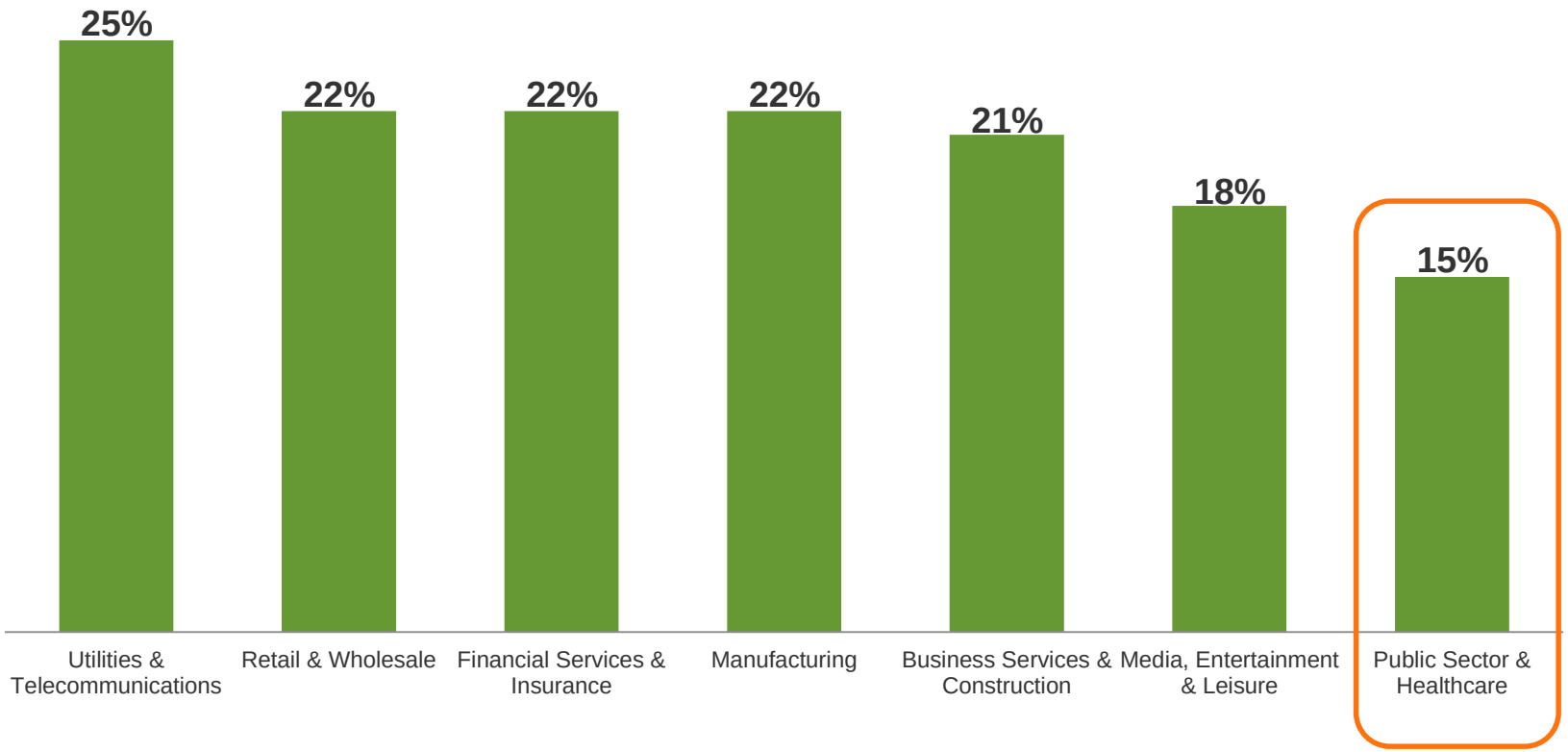
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Agenda

- *Research Overview*
- *Top 5 IT Trends Putting Healthcare Providers At Risk*
- *Top 5 Security Challenges Experienced By Providers*
- *Healthcare Security Budget Trends*
- *The Path Forward*

Healthcare Security Spending Lags Behind All Other Industries

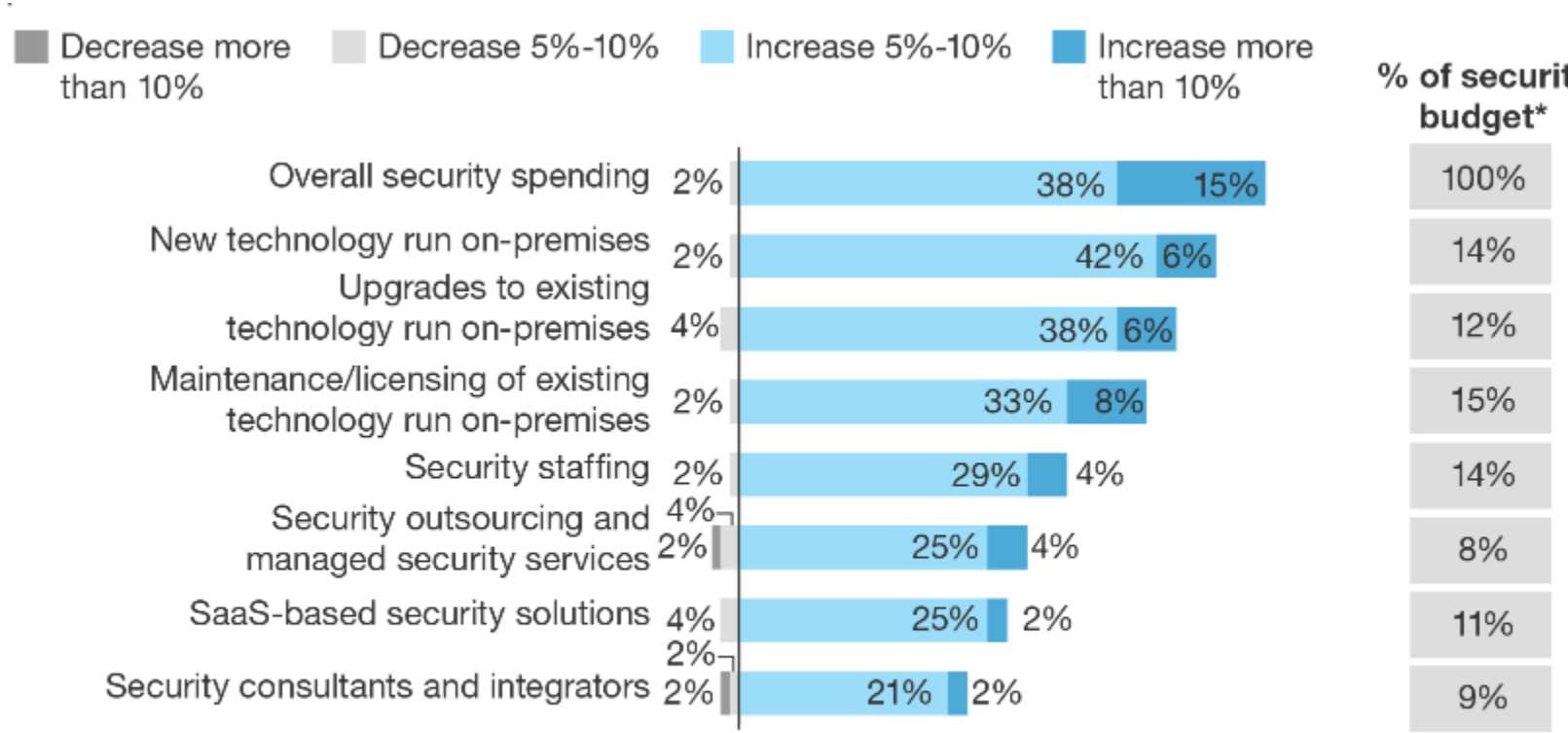
"How much does your firm's information/IT security spending for 2015 represent as a percentage of overall 2015 IT budget?"



Base: 2,698 Global security decision-makers (20+ employees) in public sector and healthcare

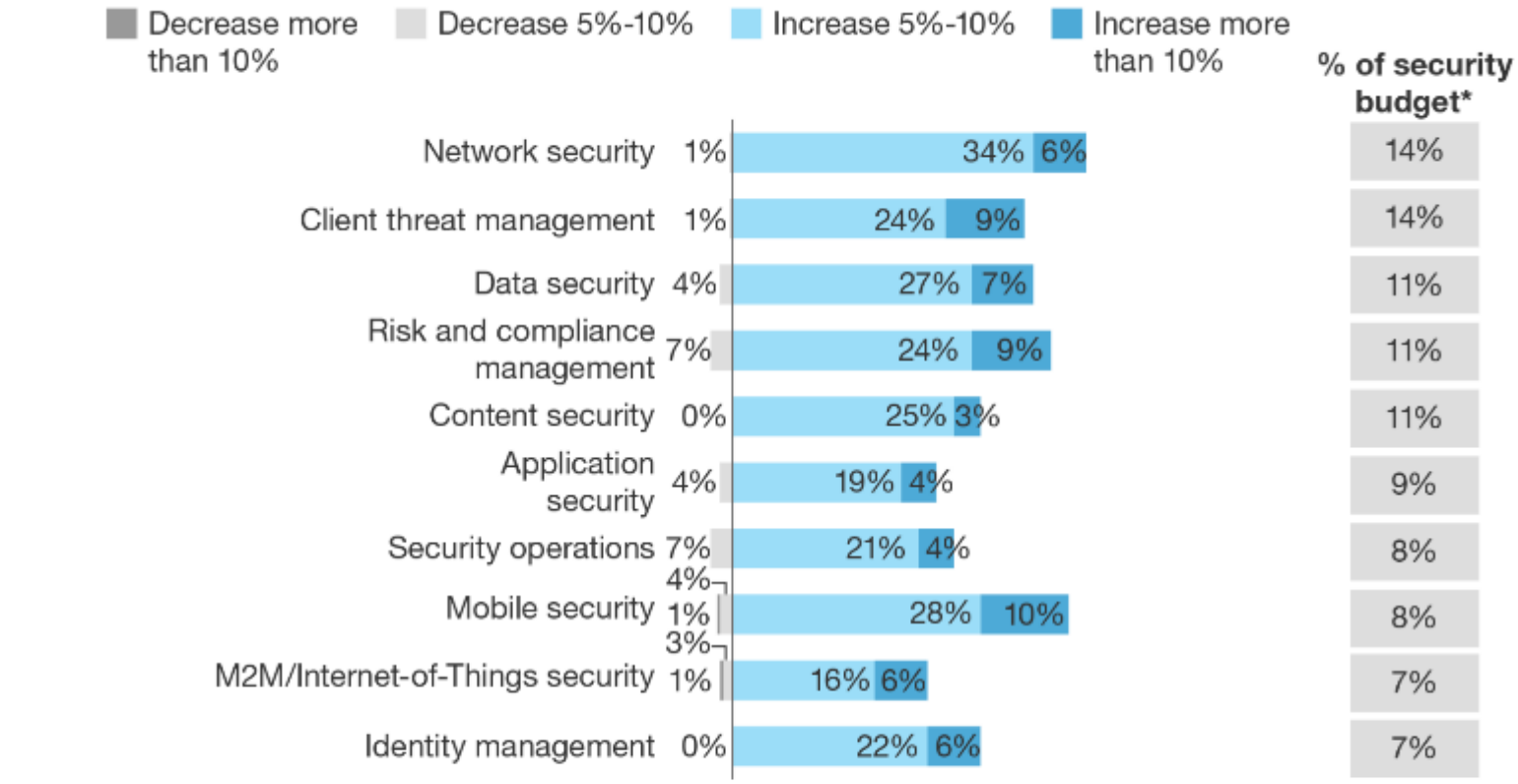
Source: Forrester's Global Business Technographics® Security Survey, 2015

Healthcare Security Programs Are Shifting Under Heavy Weight



Base: 48 US healthcare security technology decision-makers (20+ employees)
*Base: 53 US healthcare security decision-makers (20+ employees)
("don't know" and "stay about the same" not shown)

Healthcare Orgs Focus Their Security Spending On Key Functional Areas



Base: 67 US healthcare security decision-makers (20+ employees)
*Base: 35 US healthcare security technology decision-makers (20+ employees)
("don't know" and "stay about the same" not shown)
Source: Forrester's Global Business Technographics® Security Survey, 2015

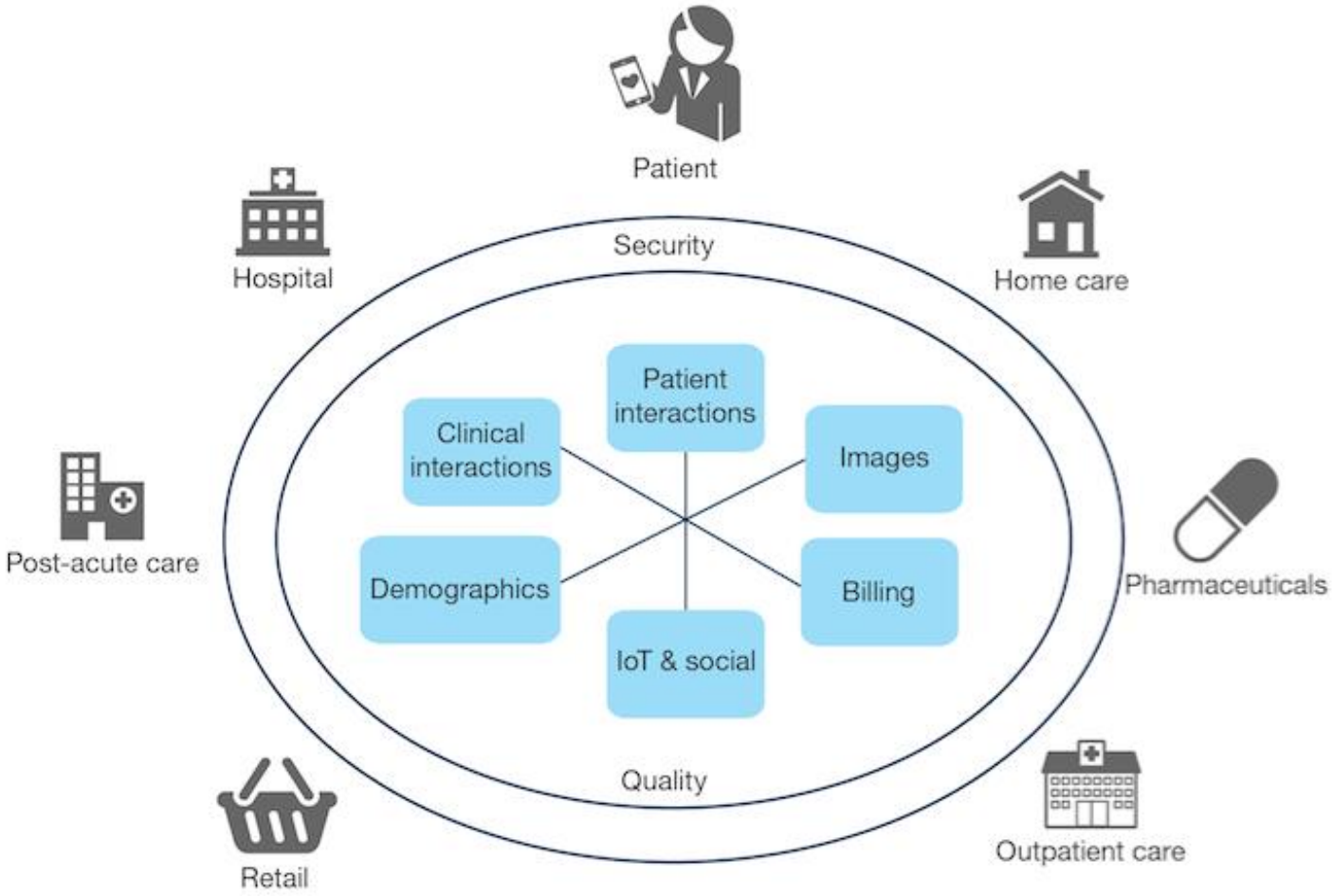
Agenda

- *Research Overview*
- *Top 5 IT Trends Putting Healthcare Providers At Risk*
- *Top 5 Security Challenges Experienced By Providers*
- *Healthcare Security Budget Trends*
- *The Path Forward*

Familiarize Yourself With The OCR's Audit Protocol

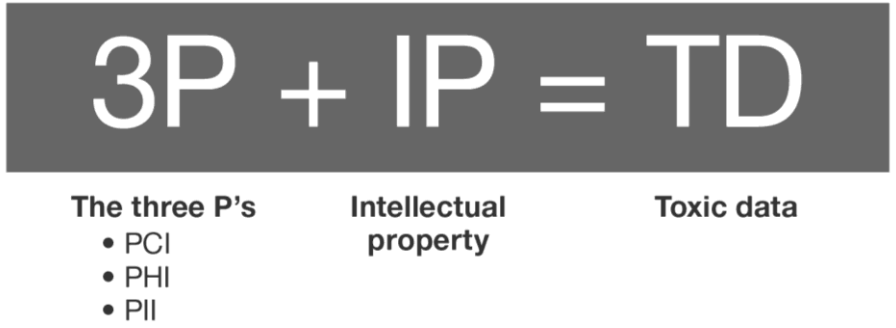
- Don't wait for the OCR to come knocking
- Perform a self assessment now
- Include medical devices in your assessment
- Evaluate your existing vendor SLAs for security gaps

Adopt A Data-Centric Security Strategy



Executing A Data-Centric Security Strategy

- Defining your data is the foundation for data security and privacy
  - Document how medical staff & data scientists are using the data
- Dynamic data classification requires both human intervention and tools
  - Classify new data first, and address legacy data later.
- Implement the appropriate controls
  - Encrypt data in-flight and at rest, regardless of location (mobile/static endpoints, servers, cloud services, medical devices)
  - Consider endpoint/network DLP



Thank you

Chris Sherman
+1 617-613-6082
csherman@forrester.com

FORRESTER®

forrester.com

6 reasons to consider Digital Guardian

1. Comprehensive data loss prevention
2. DLP < 30 minutes a day
3. Accurate & effective = lowest false positive rate
4. Integrated with leading EHRs
5. Predefined healthcare policies simplify setup
6. Trusted by 100+ healthcare systems

#1: Comprehensive Data Protection

DIGITALGUARDIAN FOR NETWORK DATA LOSS PREVENTION

DIGITALGUARDIAN FOR DATA DISCOVERY

DIGITALGUARDIAN FOR ENDPOINT COMPLIANCE

DIGITALGUARDIAN FOR CLOUD DATA PROTECTION

#2:DLP < 30 minutes a day

"Implementation is greatly simplified…with average deployment times much shorter than other DLP products. ***Implementations can often be completed in a single day****, with only minimal policy tuning required thereafter."*

- Data Loss Prevention Leading Vendors Review, DLP Experts, Jan 2016

DLPX
DATA LOSS PREVENTION EXPERTS

#2:DLP < 30 minutes a day

"I find myself spending less then 30 minutes a day with the system."

- Steve Scott, Information Security Manager, Saint Charles Health System

#3: Accurate & effective

Database Record Matching delivers unmatched PII/PHI identification and control

#4: Integrated with leading EHRs

#5: Predefined policies simplify setup

- PHI data
  - Multiple polices detect, log, encrypt, and/or block PHI
- Patient financial data
  - Multiple policies detect, log, encrypt, and/or block patient financial data
- Unencrypted EDI
  - Unencrypted HL7 and X12 messages by source and destination
  - Unsecured partner EDI communications can be easily discovered and corrected

#6: A trusted partner

DIGITAL GUARDIAN IS SUCCESSFULLY DEPLOYED IN MORE THAN 100+ HEALTHCARE SYSTEMS

Employees are your biggest risk

"Since implementing DG, we find people are much more careful with SCHS sensitive data. With this tool we don't have to be the IT Police. We can give functionality back to our users knowing that our data is being properly handled and protected."

- Steve Scott, Information Security Manager, Saint Charles Health System

DIGITAL GUARDIAN

box

On-Demand Webinar:
How a Renowned Healthcare Institution Shares Patient Data in the Cloud - Securely

Mark Menke, Principal Architect, Digital Guardian

DIGITAL GUARDIAN®

Q & A