Breach Readiness…How do you Rank?

A Joint Presentation Featuring:
Chris Logan, Sr. Healthcare Strategist, VMware;

David Houlding, Director Healthcare Privacy and Security, Intel Health and Life Sciences; and

Hussein Syed, CISO, RWJBarnabas Health

September, 2017

Healthcare, Hacked

Kristina Grifantini, MS
Writer & Editor, Southern CA

Data Breaches Cost Health Care Industry $6.2 Billion

BY: Robin Tiberio and Sarah Park Masuda

Report: Hackers Caused 98% of Healthcare Data Breaches in 2015

by Fred Pennic 01/28/2016 0 Comments

Insiders: Health care is 'being held hostage to hackers'

By **DAN DIAMOND** | 05/10/16 08:11 AM EDT

LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool

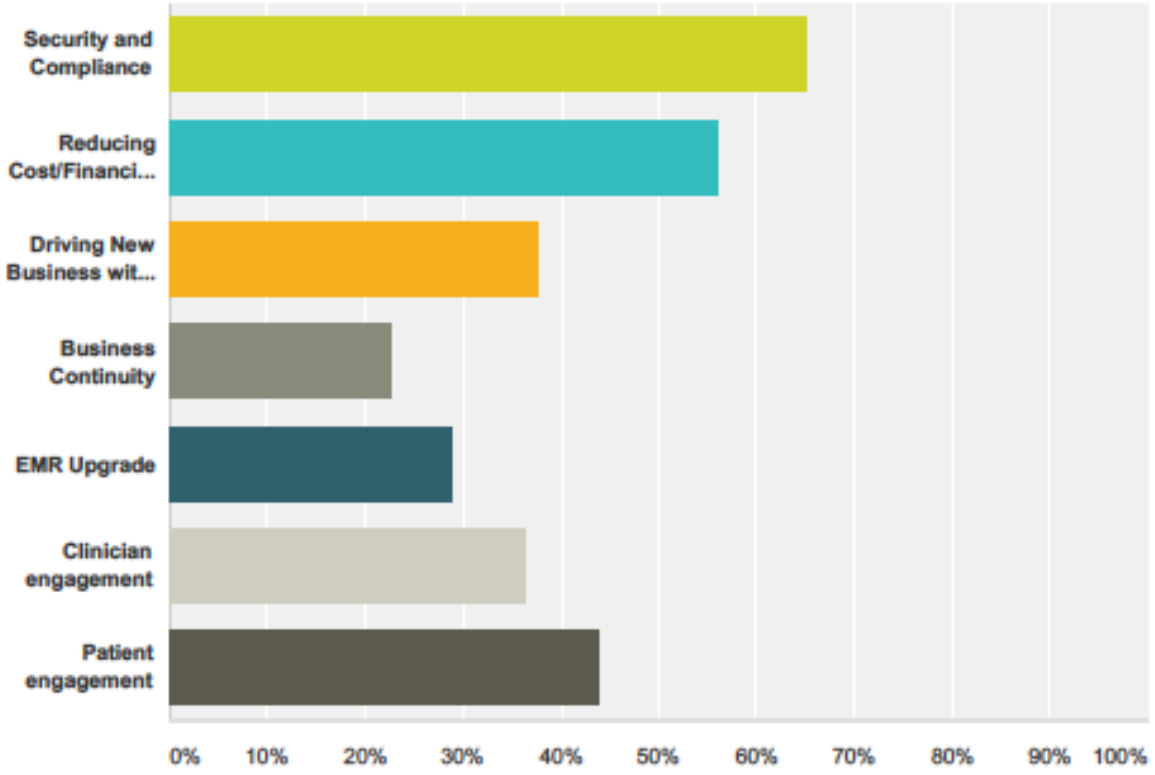
Leer en español

By **NICOLE PERLROTH** and **DAVID E. SANGER** MAY 12, 2017

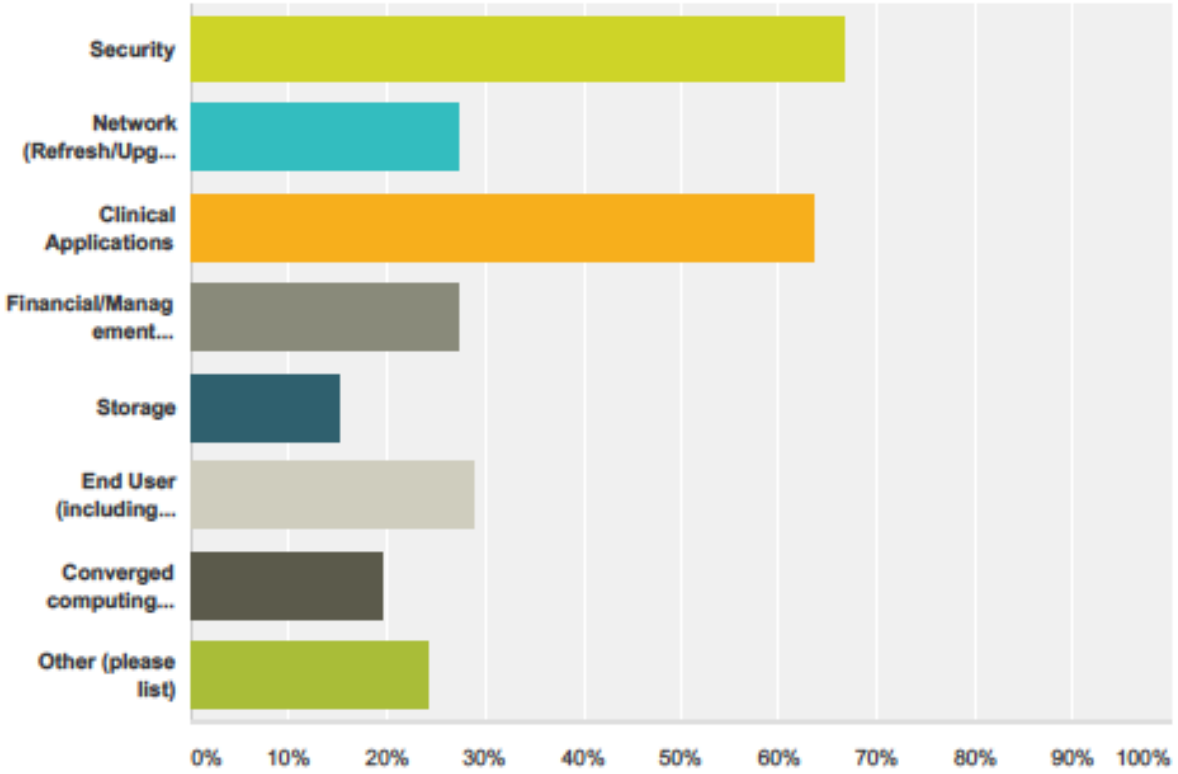
vmware

2016 College of Healthcare Information Management Executives (CHIME) Survey Results

Top Concerns for CIOs



What are you implementing this year



VMware commissioned a survey with CHIME to understand key issues for Providers related to IT and IT Services

Healthcare – Target for Attack

18% of US GDP is spent on Healthcare

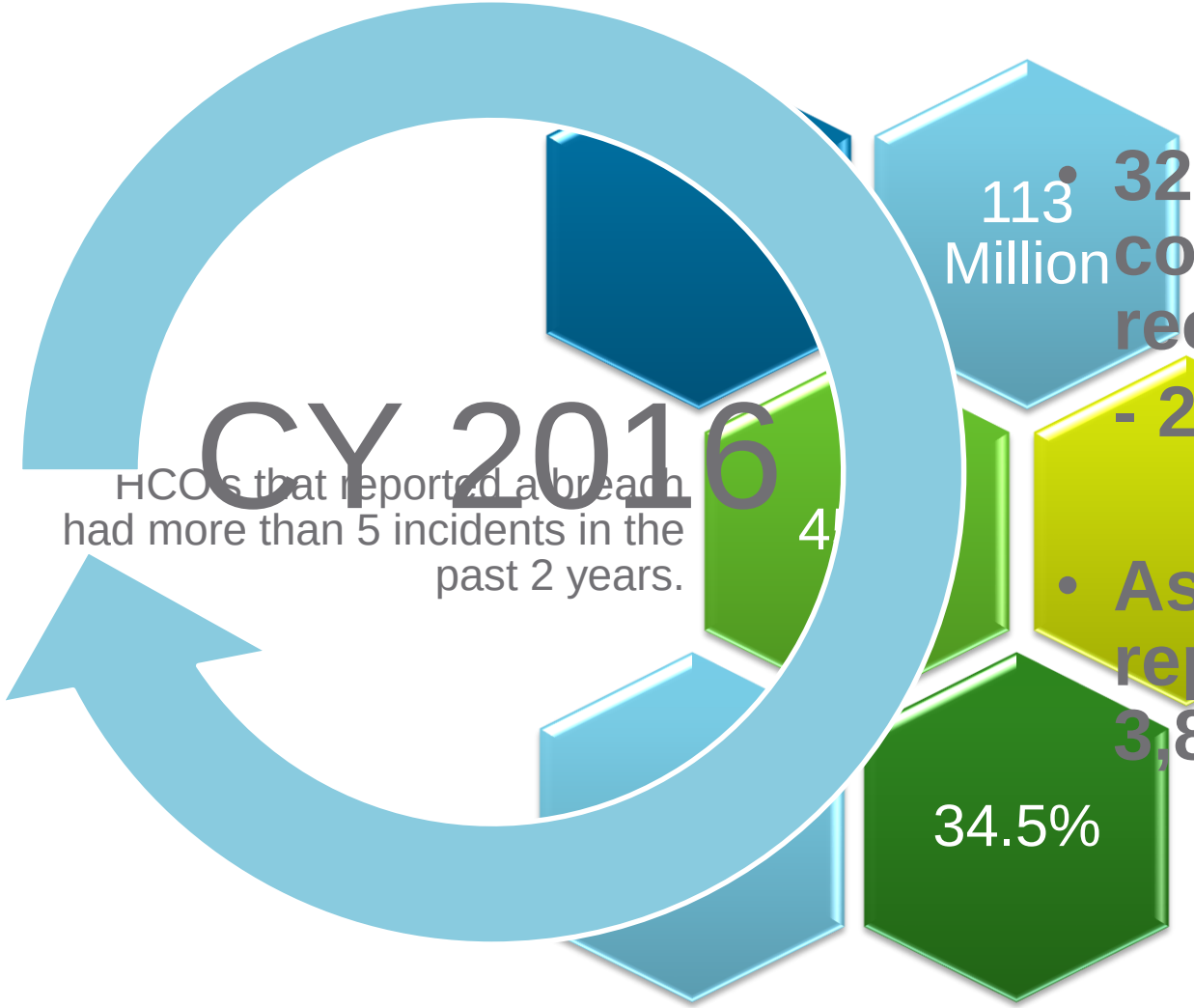
47% of US Population has had personal healthcare data compromised

90% of HCO's have experienced a breach involving the loss or theft of patient data in the past 2 years

Is Healthcare a prime target for attackers or our we just more susceptible to successful compromise?

Source: Hacking Healthcare IT in 2016: Lessons that the healthcare industry can learn from the OPM Breach. January 2016
Ponemon Institute Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, May 2016.

Data Loss at an All Time High

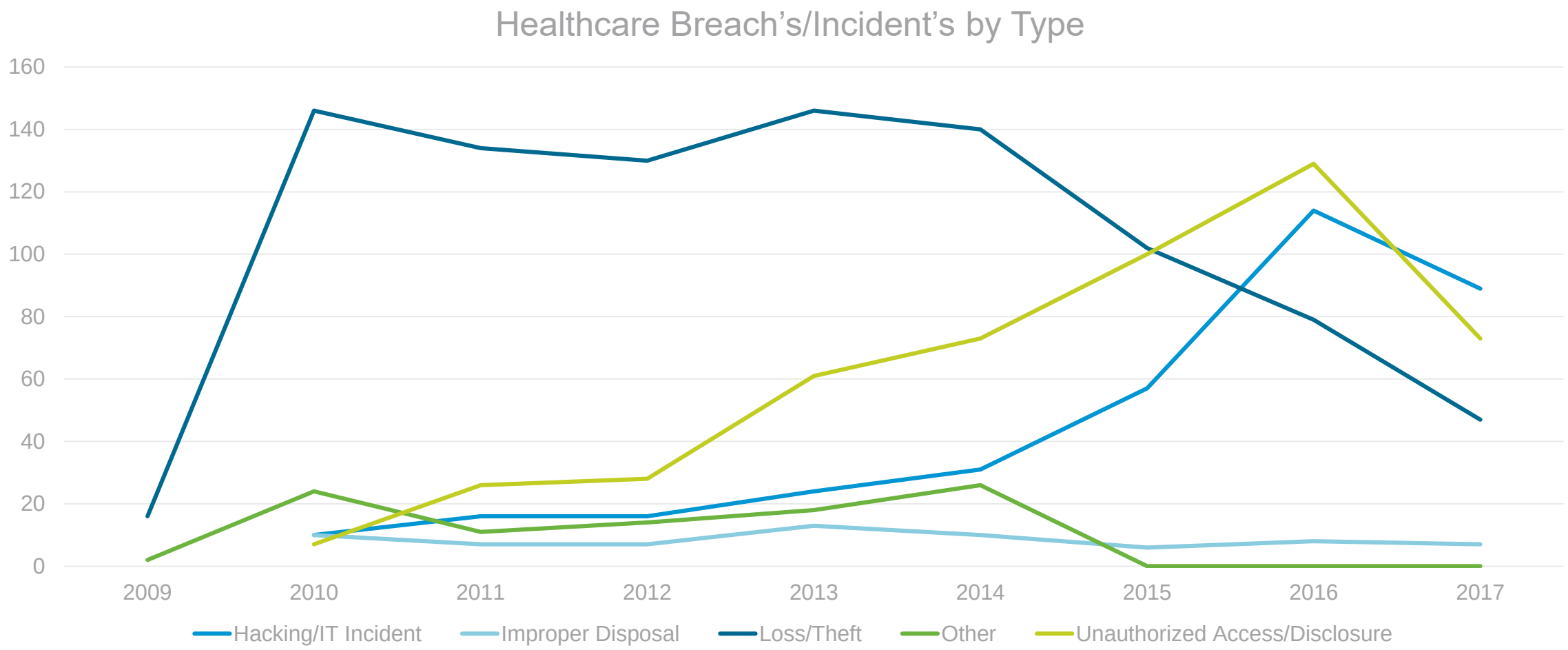


- **328 incidents and 16,655,952 compromised healthcare records**
  - Healthcare records were compromised in the U.S. (2015)
- **- 22% increase from 2015**
- **As of August 25th, 2017, 216 reported incidents and 3,821,227 compromised records**
  - Of ALL reported data breaches in 2016, were healthcare related

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

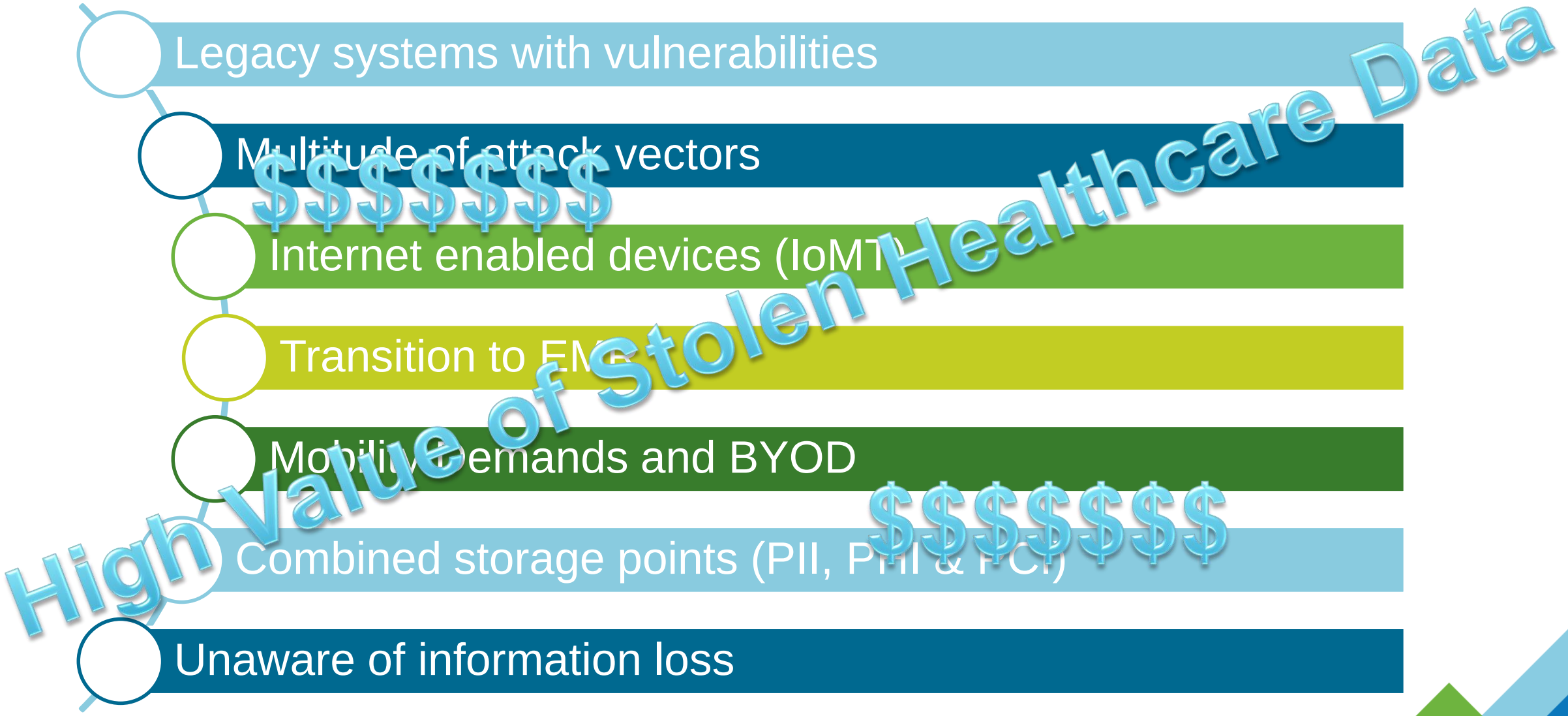
Ponemon Institute Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, May 2016.

OCR Reported Breaches Through Calendar Year 2016

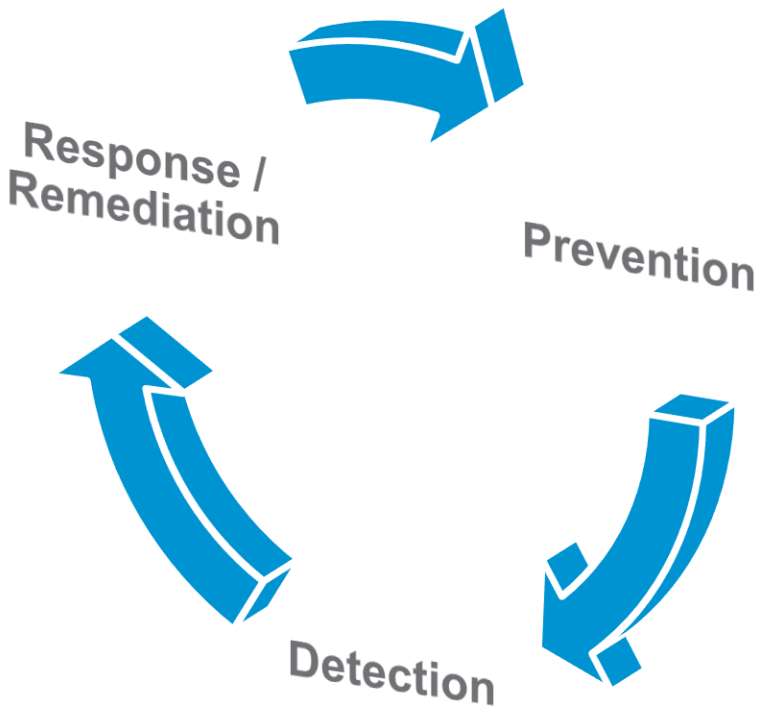


Source:https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Security Issues and Data Breaches are on the Rise…Why?



What can we do to stop the bleeding?



Prevention – Least Privileged and Awareness

Detection – Context and Visibility

Response / Remediate – Plan and Automate

Future Security Considerations for Healthcare

vmware

Future Security Considerations for Healthcare

Plan and prepare for an attack

Realize the value of medical data

There is no silver bullet for security

Cloud/Workloads are as secure as you make them

Security must harmonize with business process

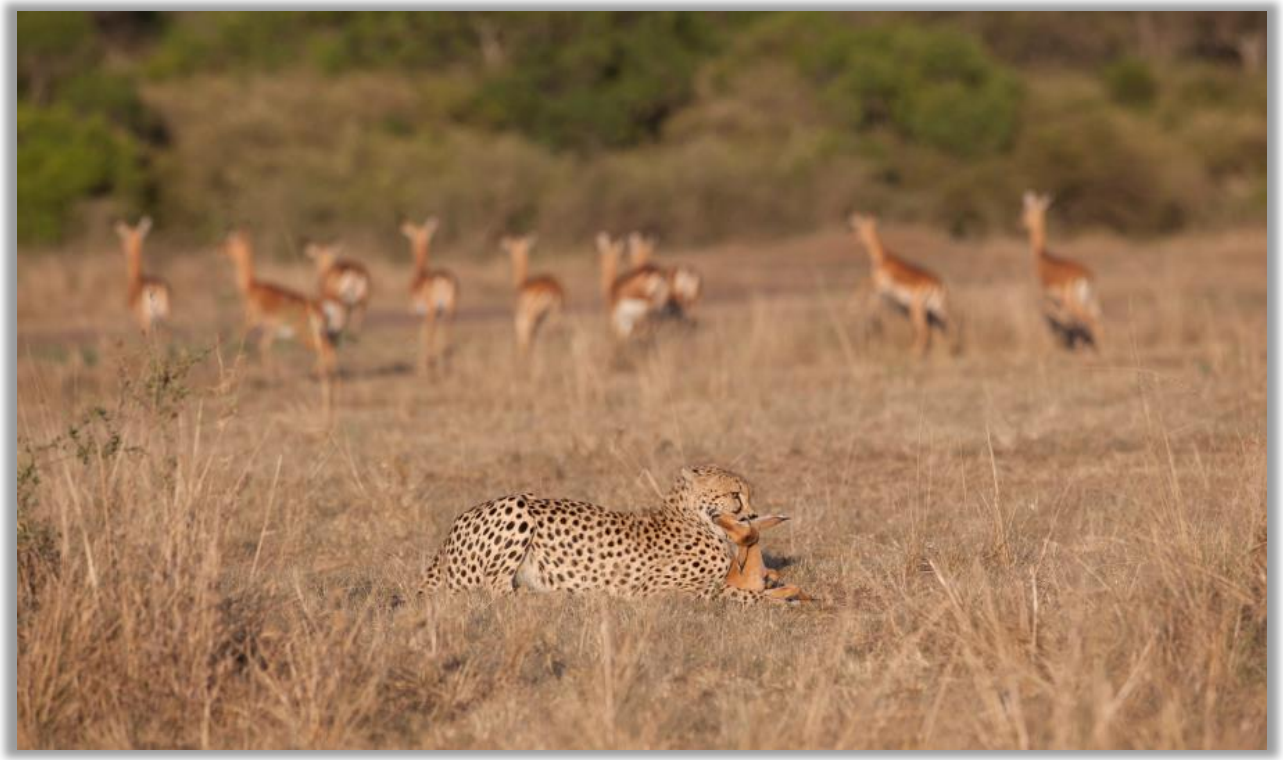
Source: http://healthitsecurity.com/news/5-healthcare-security-considerations-going-into-2016

“Success is not final, failure is not fatal: it is the courage to continue that counts.”

- Winston Churchill

Healthcare Security – Increasingly About Survival

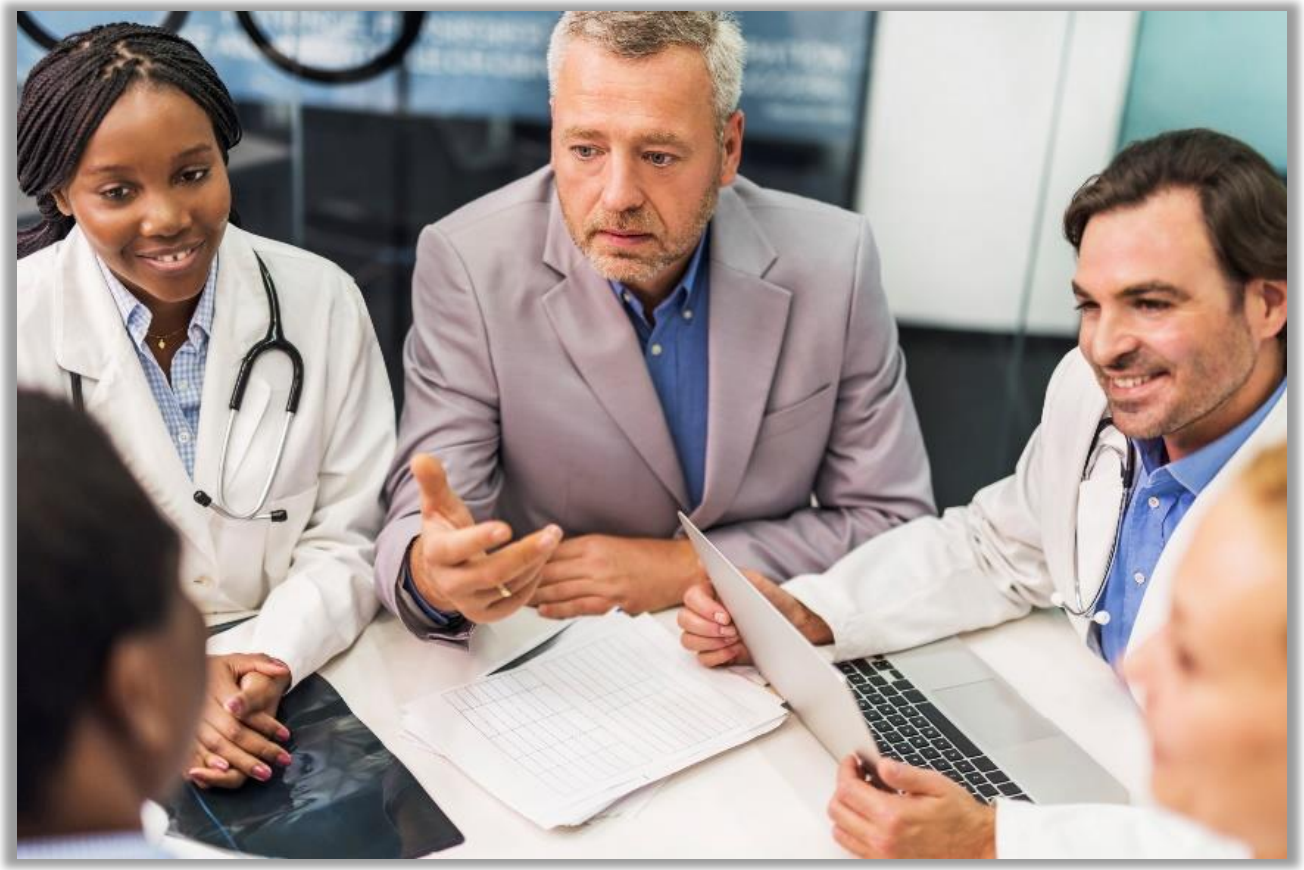
- Major impact of breaches and ransomware
- Compliance important … but not sufficient
- How far do you need to go?
- How does your security compare?



- Security Readiness Workshop
  Benchmark security against industry, peers: same locale, type, size
- See if lagging, and if so what capabilities
- Prioritize gaps, rally support to address

Global Health & Life Sciences – Industry Results

- **N=144** HLS orgs globally
- Projected to more than double through 2018
- **Providers, payers, pharma, life sciences, revenue cycle, and business associates**
- Spans **9** countries and growing
- **High quality data**
  - Trained security assessors
  - Verified security teams in HLS organizations
  - HLS organizations can update their data, i.e. kept evergreen



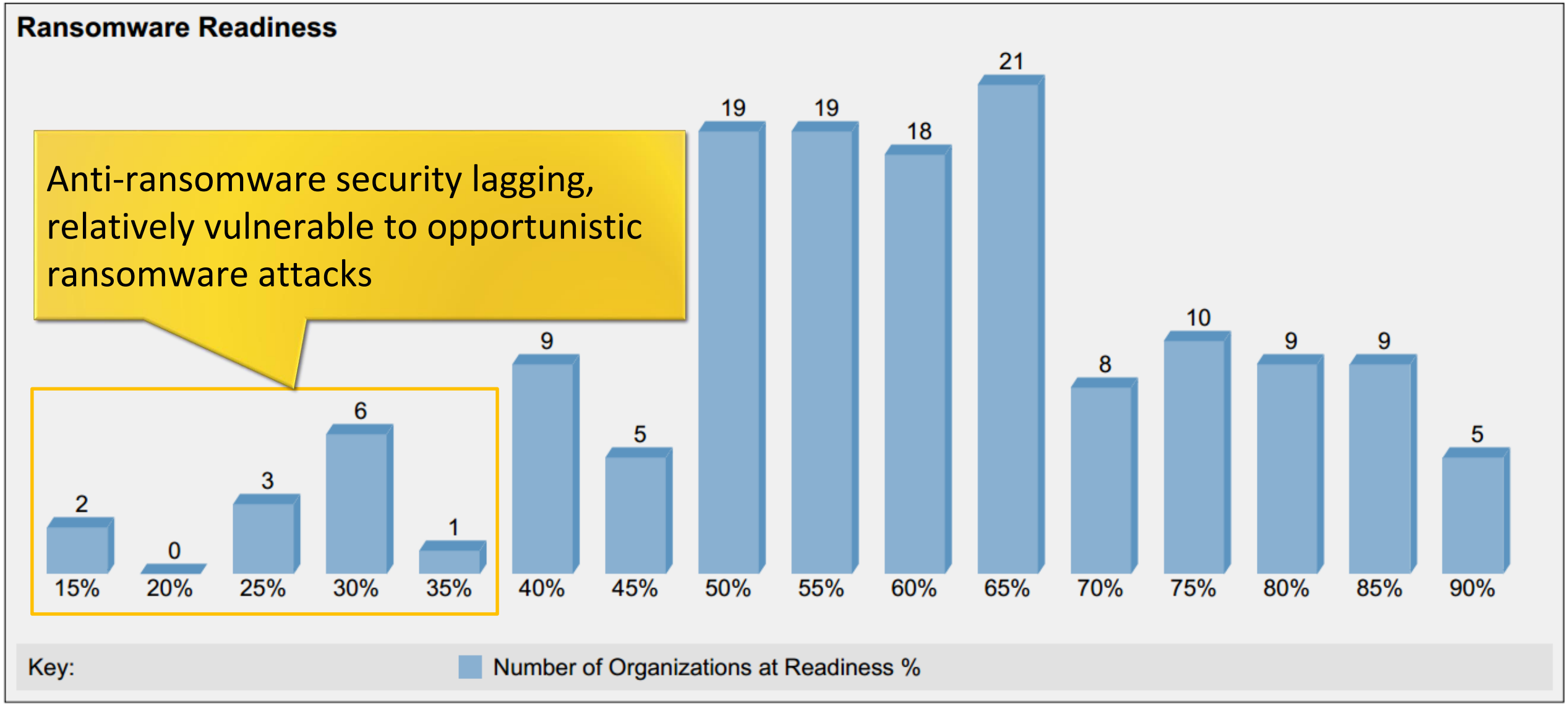
HLS Security Priorities and Readiness Results

Health and Life Sciences Industry Priorities and Readiness

#	Breach Type	Average Priority	Readiness Min	Readiness Mean	Readiness Max	Readiness Std Dev
2.1	Cybercrime Hacking	Medium / High (78%)	21%	58%	93%	15%
2.2	Loss or Theft of Mobile Device or Media	Medium (51%)	14%	51%	90%	15%
2.3	Insider Accidents or Workarounds	Medium / High (65%)	15%	54%	90%	16%
2.4	Business Associates	Medium (51%)	6%	61%	100%	21%
2.5	Malicious Insiders or Fraud	Medium (44%)	15%	52%	89%	15%
2.6	Insider Snooping	Medium (49%)	13%	50%	89%	16%
2.7	Improper Disposal	Low / Medium (36%)	0%	49%	92%	18%
2.8	Ransomware	High (85%)	17%	60%	91%	16%

Intel.com/SecurityReadiness N=144, Global Scope, Wednesday, 23 Aug 2017 11:19 PDT

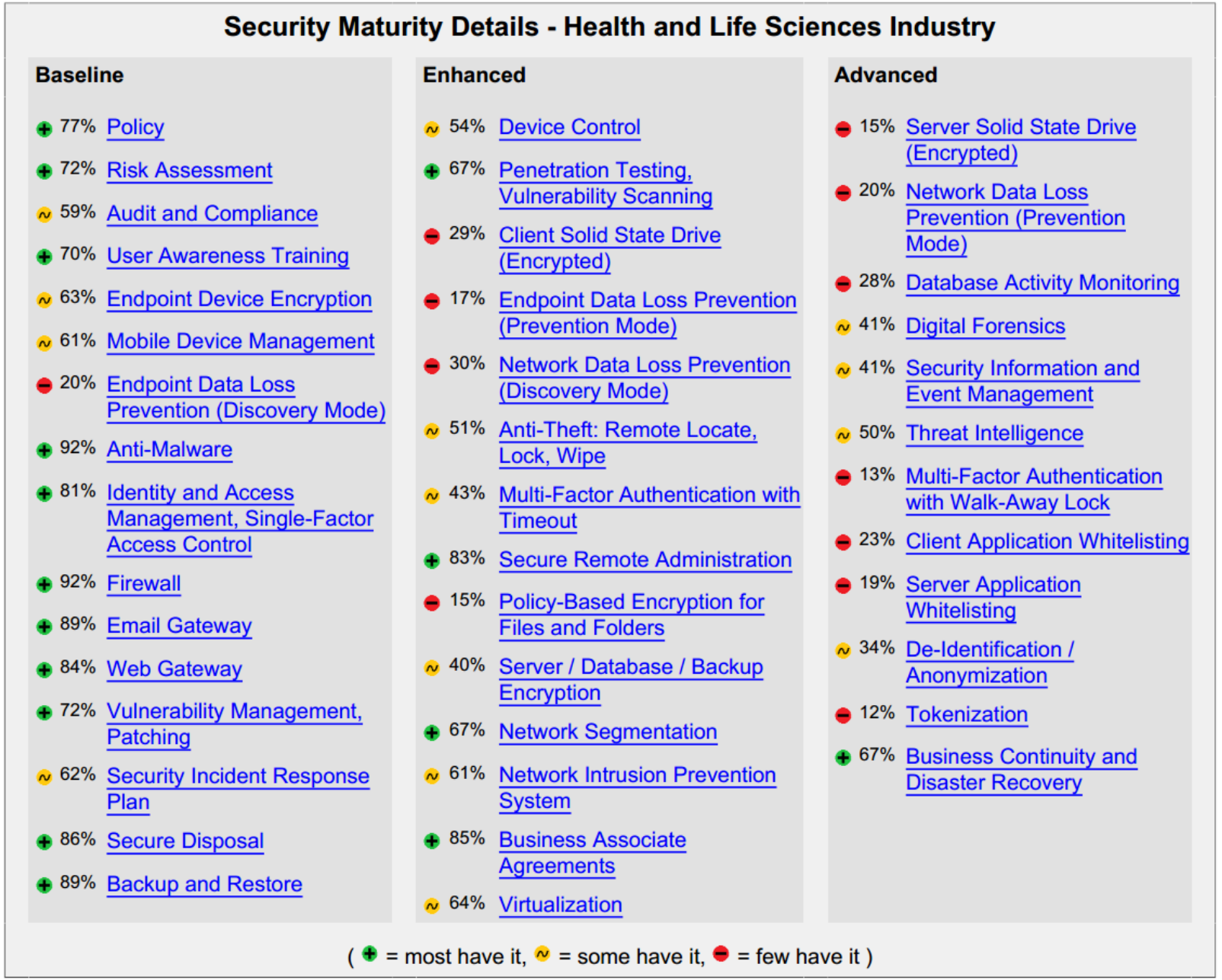
HLS Ransomware Readiness Distributions



Intel.com/SecurityReadiness N=144, Global Scope, Wednesday, 23 Aug 2017 11:19 PDT

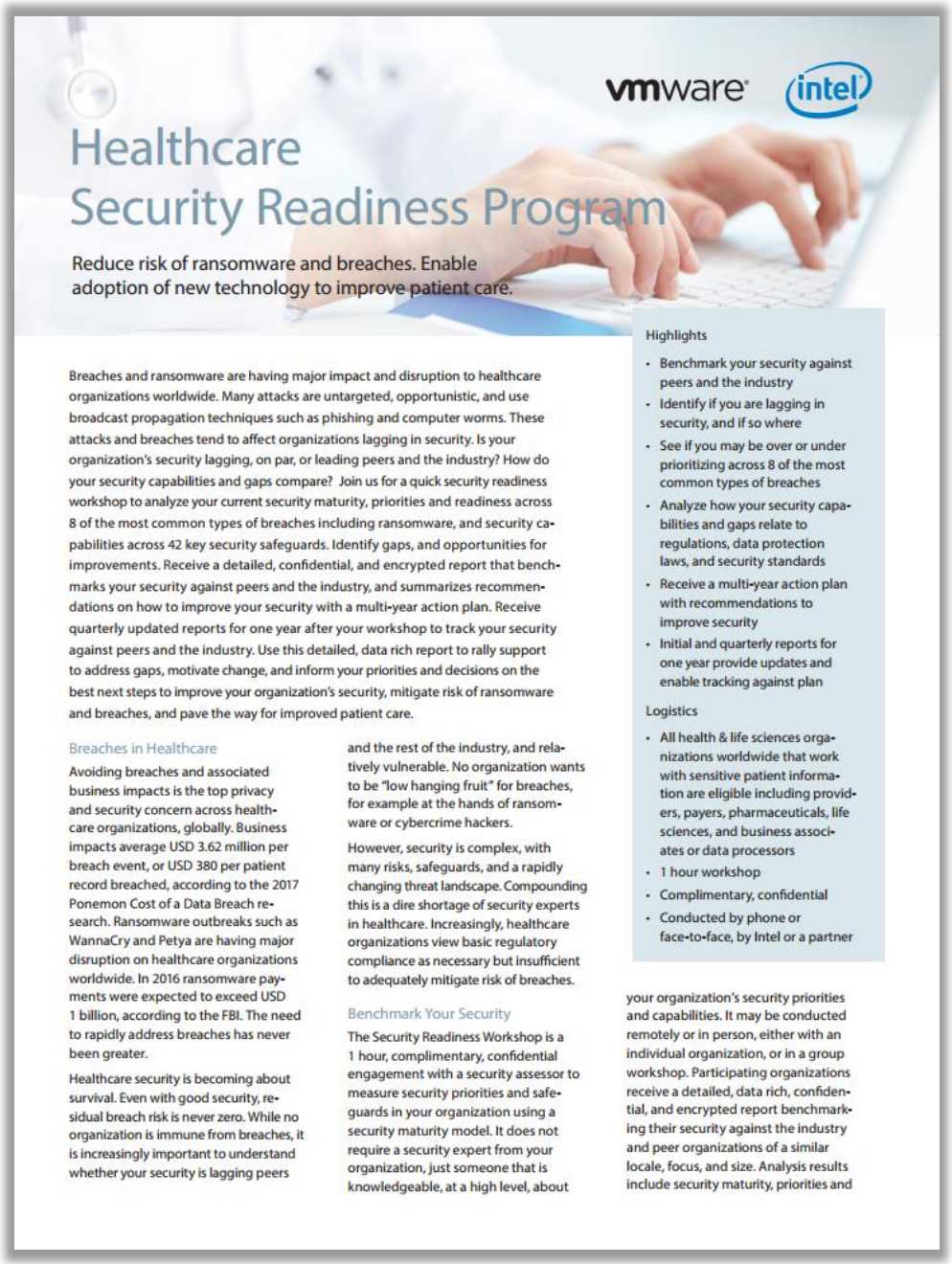
HLS Security Capabilities - Level of Implementation

- Many weak points, increasing into Enhanced and Advanced Tiers
- Move discussion to high priority breach types, specific weak points



Healthcare Security Readiness Program Brief

- Concise, 2 page overview
- 1 hour, confidential, complimentary workshop
- Conducted by Intel, VMware, or partner
- Data rich reports showing how your security compares
  - Global HLS industry
  - Peers: same region, same type, similar size
- Visit Intel.com/SecurityReadiness to download overview, sample report, latest industry results



vmware intel

Healthcare Security Readiness Program

Reduce risk of ransomware and breaches. Enable adoption of new technology to improve patient care.

Breaches and ransomware are having major impact and disruption to healthcare organizations worldwide. Many attacks are untargeted, opportunistic, and use broadcast propagation techniques such as phishing and computer worms. These attacks and breaches tend to affect organizations lagging in security. Is your organization's security lagging, on par, or leading peers and the industry? How do your security capabilities and gaps compare? Join us for a quick security readiness workshop to analyze your current security maturity, priorities and readiness across 8 of the most common types of breaches including ransomware, and security capabilities across 42 key security safeguards. Identify gaps, and opportunities for improvements. Receive a detailed, confidential, and encrypted report that benchmarks your security against peers and the industry, and summarizes recommendations on how to improve your security with a multi-year action plan. Receive quarterly updated reports for one year after your workshop to track your security against peers and the industry. Use this detailed, data rich report to rally support to address gaps, motivate change, and inform your priorities and decisions on the best next steps to improve your organization's security, mitigate risk of ransomware and breaches, and pave the way for improved patient care.

Breaches in Healthcare

Avoiding breaches and associated business impacts is the top privacy and security concern across healthcare organizations, globally. Business impacts average USD 3.62 million per breach event, or USD 380 per patient record breached, according to the 2017 Ponemon Cost of a Data Breach research. Ransomware outbreaks such as WannaCry and Petya are having major disruption on healthcare organizations worldwide. In 2016 ransomware payments were expected to exceed USD 1 billion, according to the FBI. The need to rapidly address breaches has never been greater.

Healthcare security is becoming about survival. Even with good security, residual breach risk is never zero. While no organization is immune from breaches, it is increasingly important to understand whether your security is lagging peers and the rest of the industry, and relatively vulnerable. No organization wants to be "low hanging fruit" for breaches, for example at the hands of ransomware or cybercrime hackers.

However, security is complex, with many risks, safeguards, and a rapidly changing threat landscape. Compounding this is a dire shortage of security experts in healthcare. Increasingly, healthcare organizations view basic regulatory compliance as necessary but insufficient to adequately mitigate risk of breaches.

Benchmark Your Security

The Security Readiness Workshop is a 1 hour, complimentary, confidential engagement with a security assessor to measure security priorities and safeguards in your organization using a security maturity model. It does not require a security expert from your organization, just someone that is knowledgeable, at a high level, about your organization's security priorities and capabilities. It may be conducted remotely or in person, either with an individual organization, or in a group workshop. Participating organizations receive a detailed, data rich, confidential, and encrypted report benchmarking their security against the industry and peer organizations of a similar locale, focus, and size. Analysis results include security maturity, priorities and

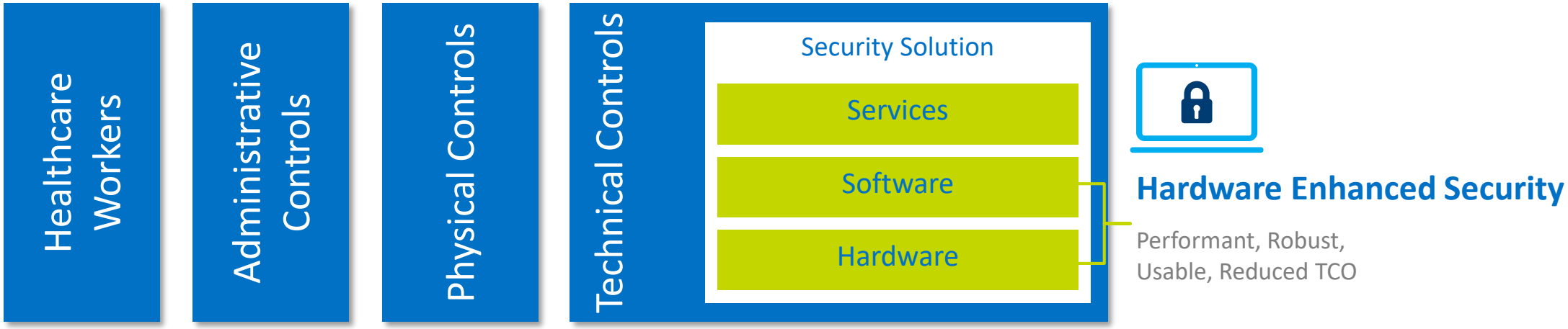
Highlights

- Benchmark your security against peers and the industry
- Identify if you are lagging in security, and if so where
- See if you may be over or under prioritizing across 8 of the most common types of breaches
- Analyze how your security capabilities and gaps relate to regulations, data protection laws, and security standards
- Receive a multi-year action plan with recommendations to improve security
- Initial and quarterly reports for one year provide updates and enable tracking against plan

Logistics

- All health & life sciences organizations worldwide that work with sensitive patient information are eligible including providers, payers, pharmaceuticals, life sciences, and business associates or data processors
- 1 hour workshop
- Complimentary, confidential
- Conducted by phone or face-to-face, by Intel or a partner

HLS Privacy & Security and Hardware Enhanced Security



Business Needs

Data Inventory, Classification, Usage, Laws / Regulations, Privacy Principles, Standards

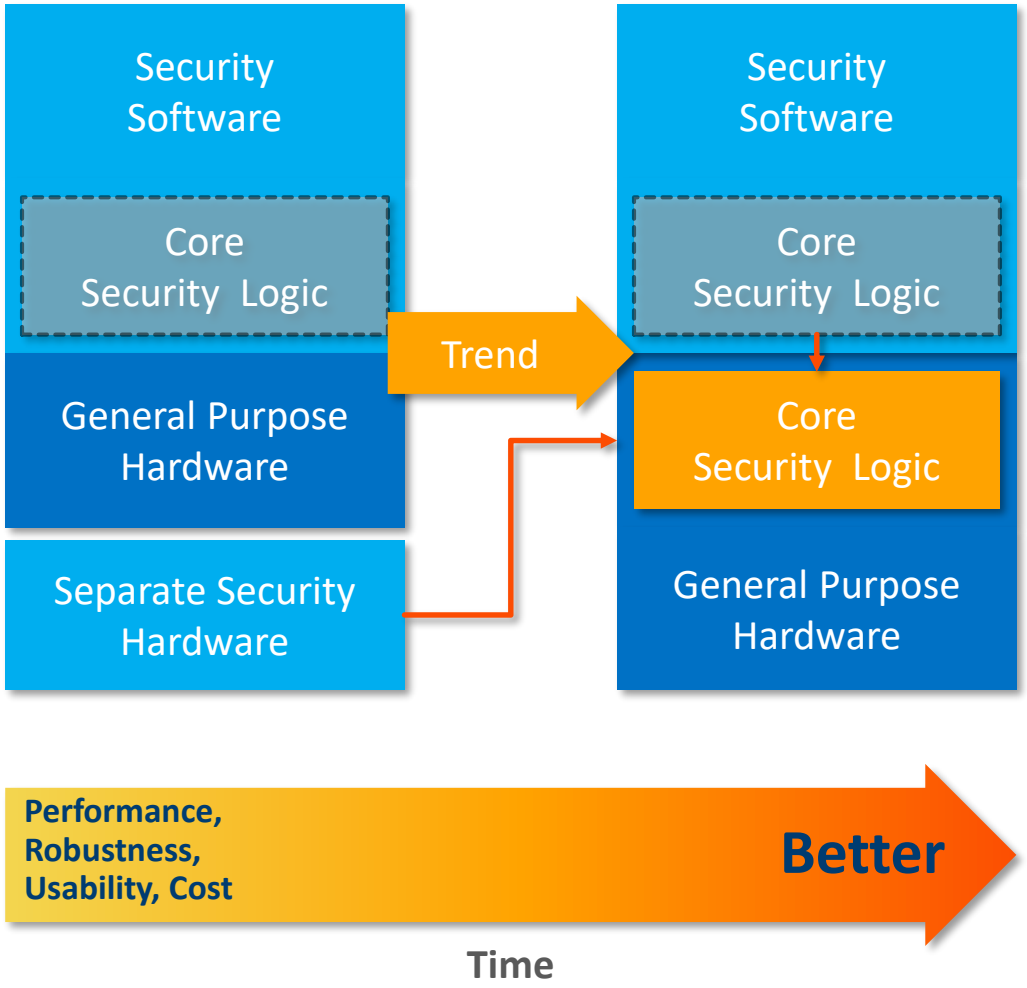
Policy

Security & Privacy Foundation in the Healthcare Organization

Risk Assessment

Identification of Security Controls Needed in the Healthcare Organization

Hardware Enhanced Security

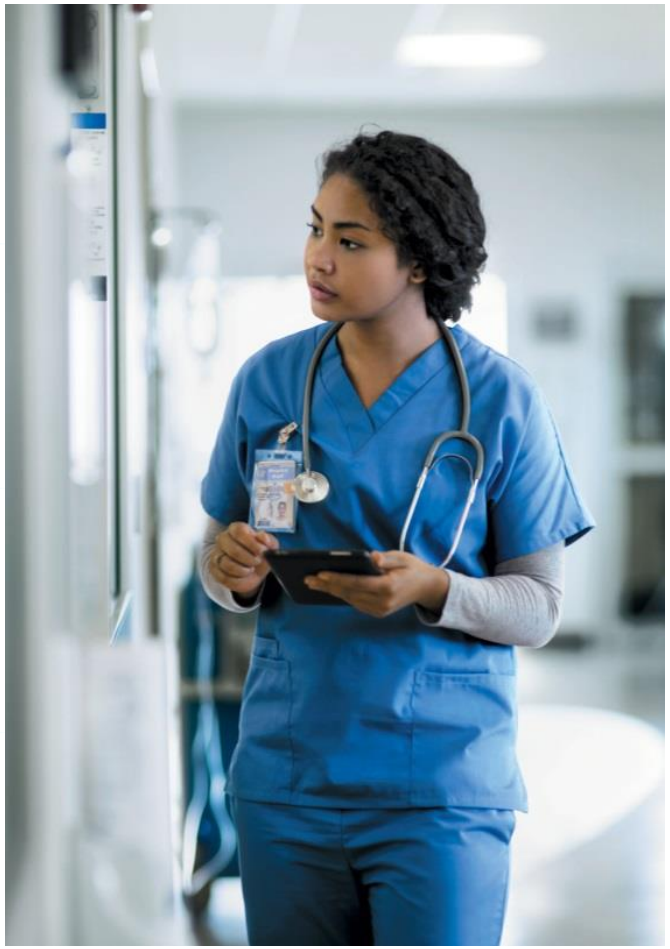


Improved usability

Hardened

Reduced Cost

Across the compute continuum



Invitation: Security Readiness Workshop

1. Benchmark your security
2. Maturity, Priorities, Readiness, Capabilities
3. Compared to HLS industry, peers of same locale, type, size
4. Maps gaps to HIPAA, NIST, PCI DSS, CIS, GDPR, ISO2700x, ISO80001, EU MDR

- 1 hour, complimentary, confidential
- See lagging, and if so what capabilities
- See how priorities compare, if over / under
- Prioritize gaps, rally support to address
- Enable proactive remediation, mitigate risk

Learn more, sign up at: VMware.com/Go/HCSecurityReadiness

Legal Disclaimers

This health & life sciences security assessment is a high-level survey of potential security issues. It is intended to inform participants about where they stand on selected security practices in relation to other similar participants in this study. It is not intended to replace participants' other compliance or security due diligence activities. It is also different from and complementary to risk assessments that are required by several regulations and security standards. It provides an opportunity to look at gaps and next steps that can be taken to improve security posture. Improvements to security based on this assessment may also help with compliance with privacy and security regulations, data protection laws, and standards. Please consult publicly available information on your applicable regulations, laws, and standards for further information.

No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

OK for Non-NDA Disclosure

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Perspective from the Field

Hussein Syed – CISO RWJBarnabas Health

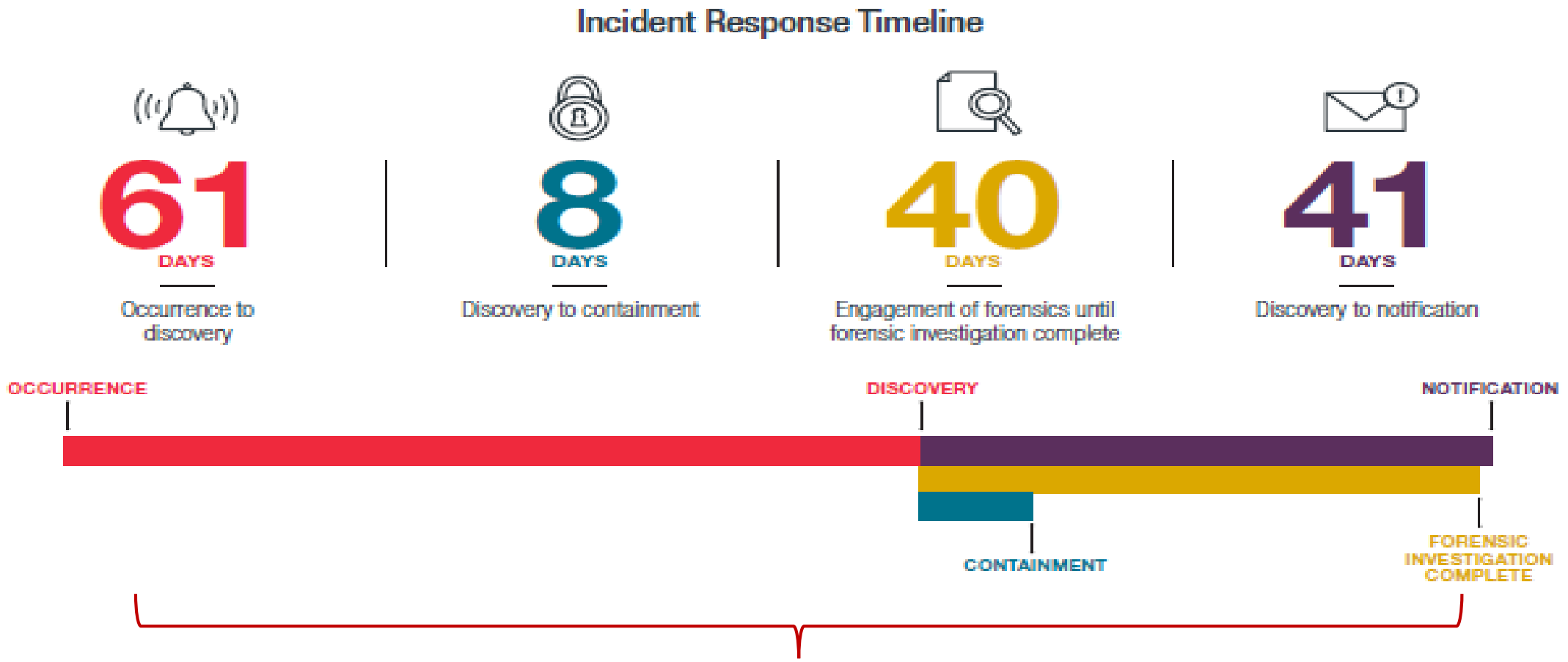
vmware

VALUE OF MEDICAL DATA and OCR FINES

- OCR fines are on the rise
- Average fine is $2.5MM
- Highest fine in 2017 gas been $5.5MM
- **A $1MM fine actually has a revenue impact of $20MM**
- **Reputation damage is not quantifiable**

vmware

Incident Response Timeline

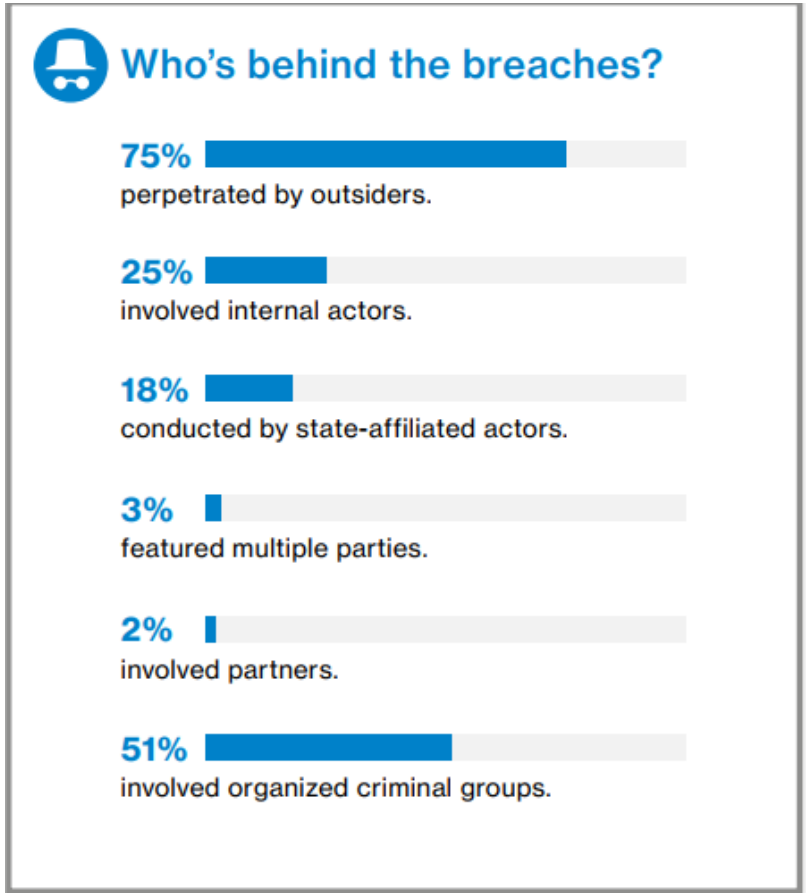


102 Days of non productive work

BakerHostetler -- 2017 Data Security Incident Response Report

Healthcare Breach Security Assessment – Perspective from the Field

- The Assessment focuses on a key area of security program. i.e. Breach Risk
- Lets you assess Baseline, Enhanced, and Advanced controls
- Shifts the perspective from traditional risk assessment
- Identifies areas to focus for breach risk



Verizon DBIR 2017

Covers Cyber Risk – Perspective from the Field

- Goes beyond HIPAA, includes controls for PCI DSS, CIS Controls and Cyber Security Framework

- Identify Cyber security exposures such as risk of Advanced Persistence Threats and Ransomware

BECKER'S HEALTH IT & CIO REVIEW

Hospitals are hit with 88% of all ransomware attacks

- The attacks targeted small to large health systems
- Average impact to an organizations is over 3 weeks to recover

Thank You!

Chris Logan, Sr. Healthcare Strategist, VMware Healthcare
clogan@vmware.com

David Houlding, Director Healthcare Privacy and Security, Intel Health and Life Sciences
david.houlding@intel.com

Husein Syed, CISO, RWJBarnabas
Hussein.Syed@rwjbh.org

vmware