



# Hospital Leaders' Guide to Cybersecurity Risk Management and Response

October 5, 2016



Our vision is of a society of healthy communities where all individuals reach their highest potential for health



Advocacy Issues Performance Improvement Research & Trends Products & Services

Home »

Like 3 Tweet Pin It Share 9

### Cybersecurity

Cybersecurity vulnerabilities and intrusions pose risks for every hospital and its reputation. While there are significant benefits for care delivery and organizational efficiency from the expanded use of networked technology, Internet-enabled medical devices and electronic databases for clinical, financial and administrative operations, networked technology and greater connectivity also increase exposure to possible cybersecurity threats that require hospitals to evaluate and manage new risks. Hospitals can prepare and manage such risks by viewing cybersecurity not as a novel issue but rather by making it part of the hospital's existing governance, risk management and business continuity framework. Hospitals also will want to ensure that the approach they adopted remains flexible and resilient to address threats that are likely to be constantly evolving and multi-pronged.

## CYBERSECURITY RESOURCES

### AHA Resources

- ▶ [A message from the AHA on cybersecurity: What hospitals need to know about ransomware, AHA News, February 22, 2016](#)
- ▶ [Audiocast: Cybersecurity education as a tool for risk management/reduction in health care organizations, February 2016](#)
- ▶ [Factsheet: Hospitals Implementing Cybersecurity Measures, January 2016](#)
- ▶ [A message from the AHA on cybersecurity: For Better Cybersecurity, Share and Share Alike, AHA News, February 2, 2015](#)
- ▶ [A message from the AHA: Considering Unique Cybersecurity Risks of Medical Devices is Critical, AHA News, December 4, 2014](#)
- ▶ [Audiocast Series - Cyber 911: Responding to a Cybersecurity Breach, December 2014](#)
- ▶ [Replay for Town Hall Interactive Webcast held November 12, 2014](#)
- ▶ [Cybersecurity and Hospitals: What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response \(August 2014\)](#)
- ▶ [Cybersecurity and Hospitals: Four Questions Every Hospital Leader Should Ask In Order To Prepare for and Manage Cybersecurity Risks](#)
- ▶ [Top Six Actions to Manage Hospital Cybersecurity Risks](#)
- ▶ [AHA Member Webinar Series - Cybersecurity for Healthcare Leaders](#)
- ▶ [AHA Regulatory Advisory: Cybersecurity Framework for Improving Critical Infrastructure](#)

### Comment Letters and Other Policy-Related Documents

- ▶ [AHA Views on the Framework for Improving Critical Infrastructure Cybersecurity, February 9, 2016](#)
- ▶ [AHA to FDA Re: Collaborative Approaches for Medical Device and Healthcare Cybersecurity, November 21, 2014](#)
- ▶ [AHA Comments to Dept. of Commerce Re: The Preliminary Cybersecurity Framework](#)

**Search**

**AHA MEMBERS-ONLY RESOURCES**

[Click here for AHA Members-only Resources.](#)

**IMPORTANT CYBERSECURITY ALERTS**

[OCR Offers Advice to Assist HIPAA-Covered Entities Avoid Ransomware \(Feb. 3, 2016\)](#)

[FDA Guidance for Manufacturers: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf \(OTS\) Software \(July 2015\)](#)

[Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication \(May 13, 2015\)](#)

[The Industrial Control Systems Cyber Emergency Response Team \(ICS-CERT\)](#)

**Health Care-Related Messages**

[DHS issues alert related to end of support for Windows 2003 Operating System \(11/10/14\)](#)

**HITRUST Cyber Threat Intelligence and Incident Coordination Center Alert: Bash/Shellshock Vulnerability (9/25/14)**

[DHS issues guidance on Internet Explorer vulnerability \(4/30/14\)](#)

www.aha.org/cybersecurity



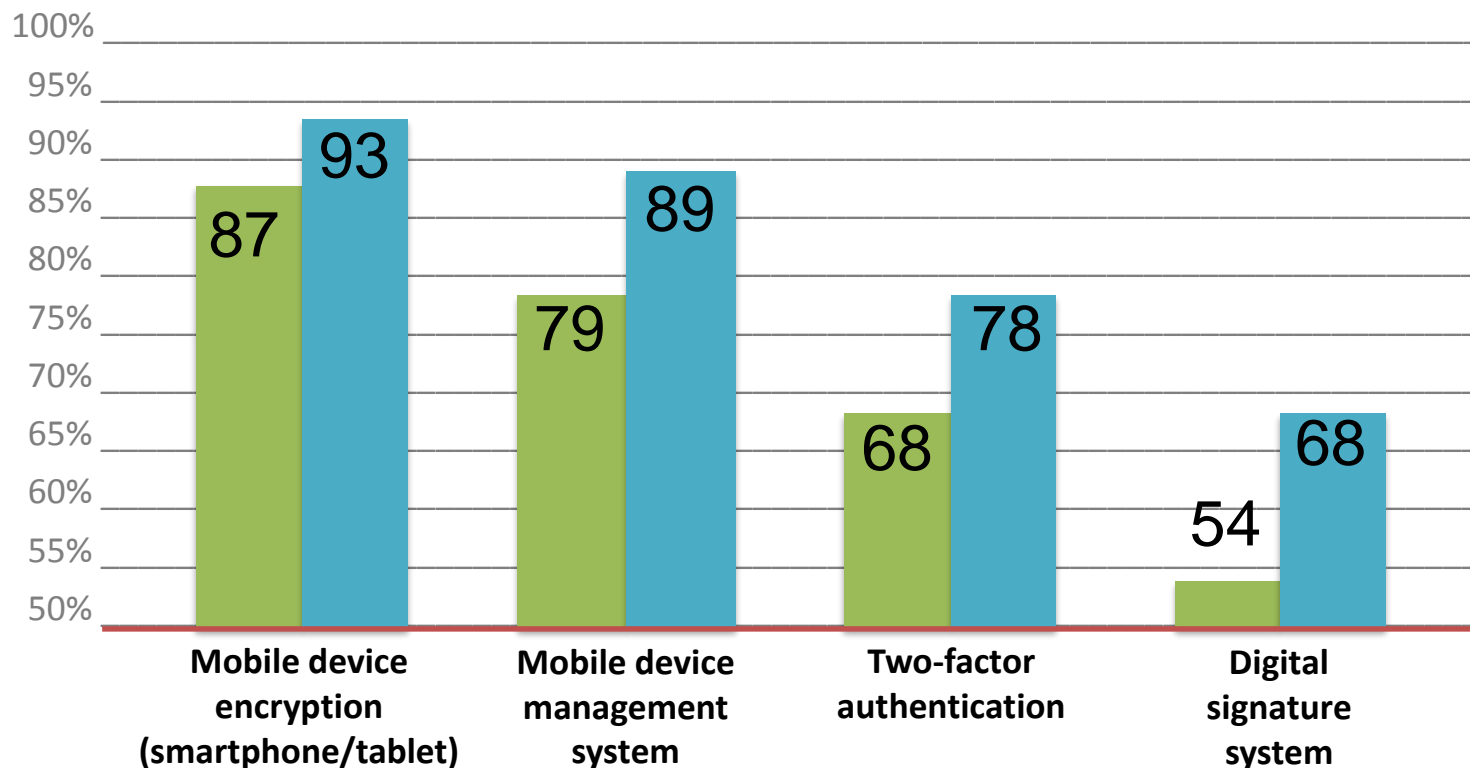
# SECURITY ASSESSMENT DATA



from the 2016  
Most Wired Survey

HealthCare's  
**most  
wired**®

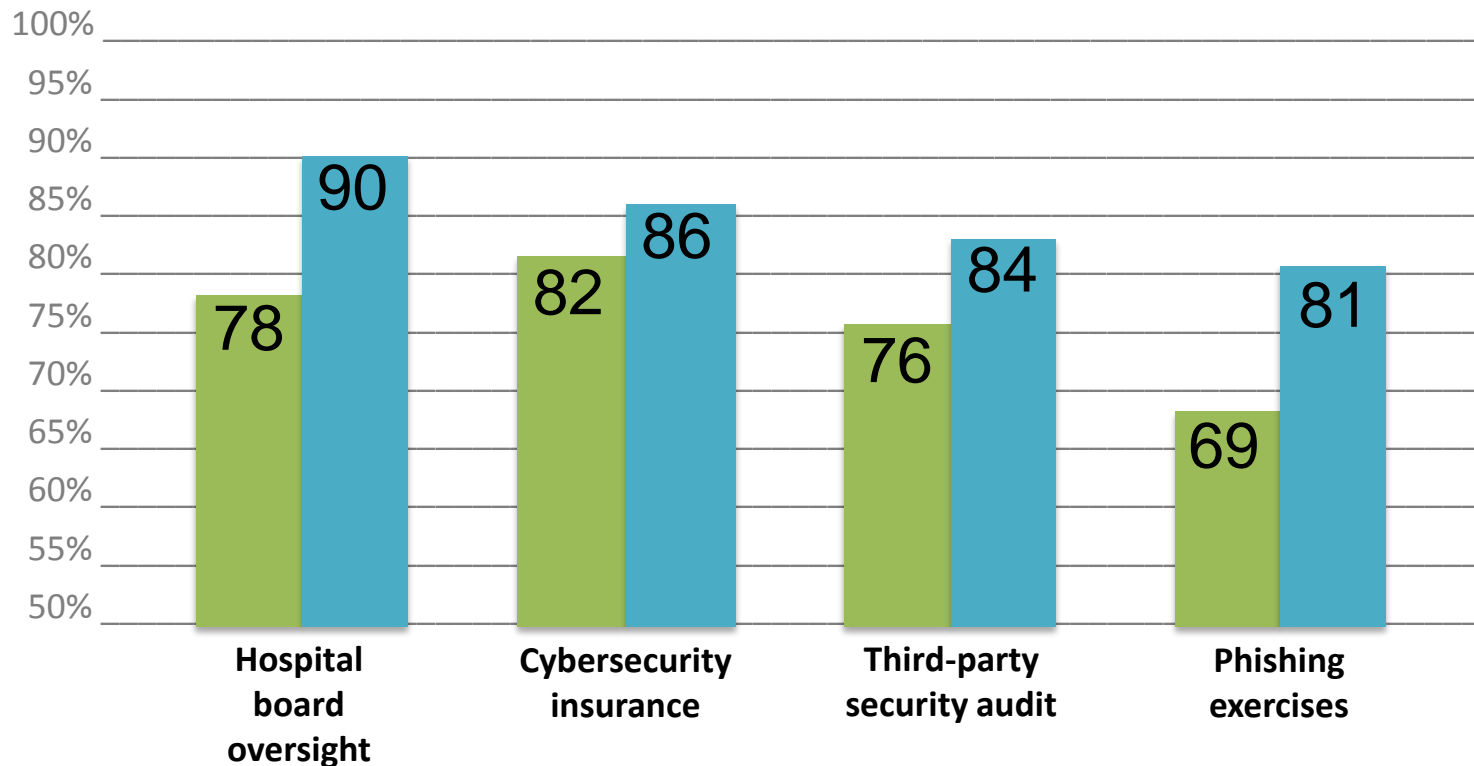
# Top growth areas in security systems



(Percent of hospitals with function enabled)



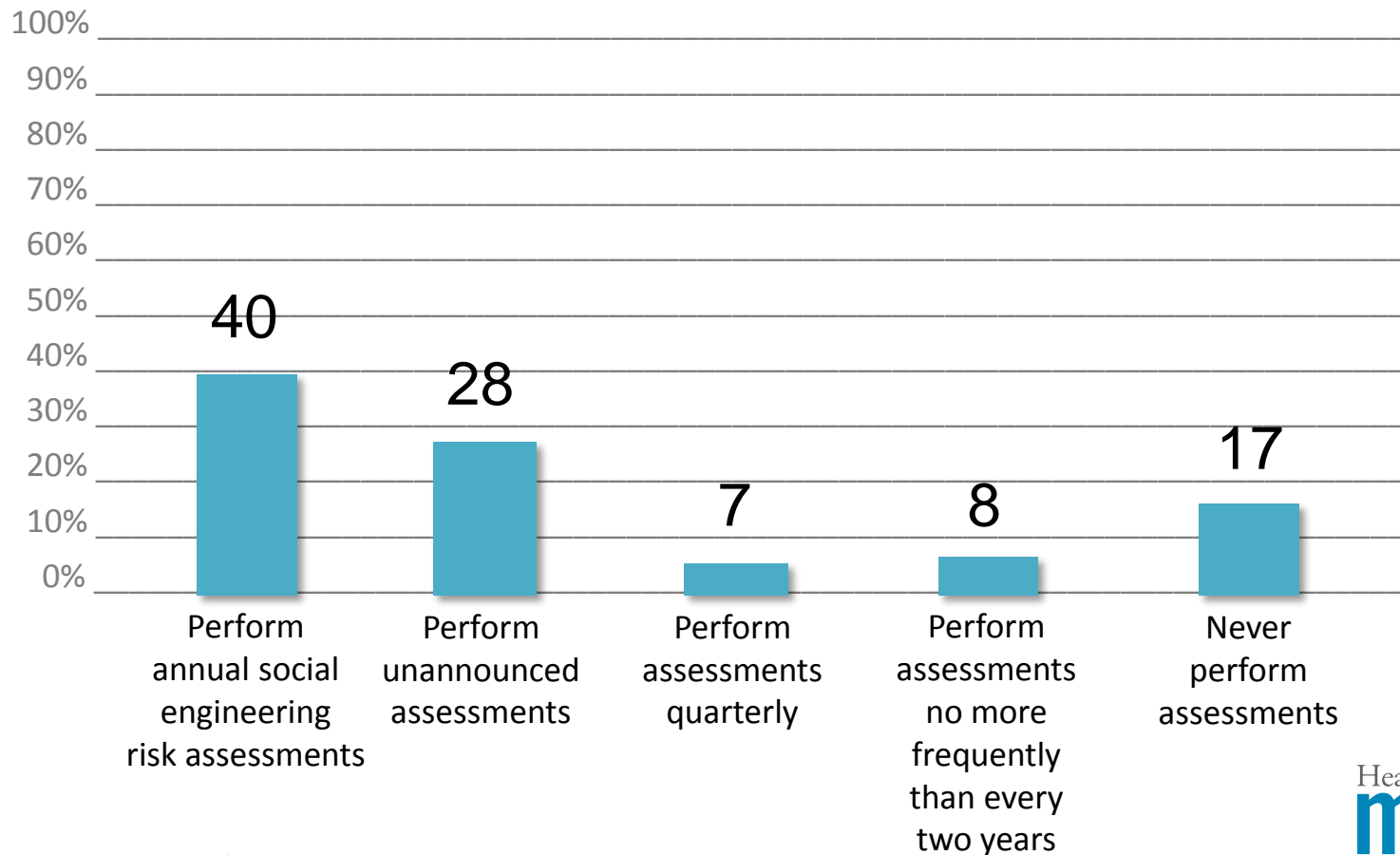
 All Most Wired survey respondents  
 2016 Most Wired

# Cybersecurity risk initiatives



 All Most Wired survey respondents  
 2016 Most Wired

# Work still to be done among the Most Wired



2016 Most Wired

# **Understanding Cyber Risks And How Your Hospital Can Confront Them**

**Ryan Spelman  
Senior Director,  
Center for Internet  
Security**

# Center for Internet Security

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities.



Criminals are targeting your organization...

Why?

Because that's how they can get to the data...



Why data?

Because that's where the money is!

# What Is The Risk?

$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Cost}$

# Threats



Yahoo

Over  
500,000,000

# Some Frightening Figures



Nearly 1 million new malware threats released every day

34.2% of user computers were subjected to at least one web attack over the year

600,000 Facebook accounts are compromised everyday

# The Only IT Field With An Adversary

Cyber Criminals



Hacktivists



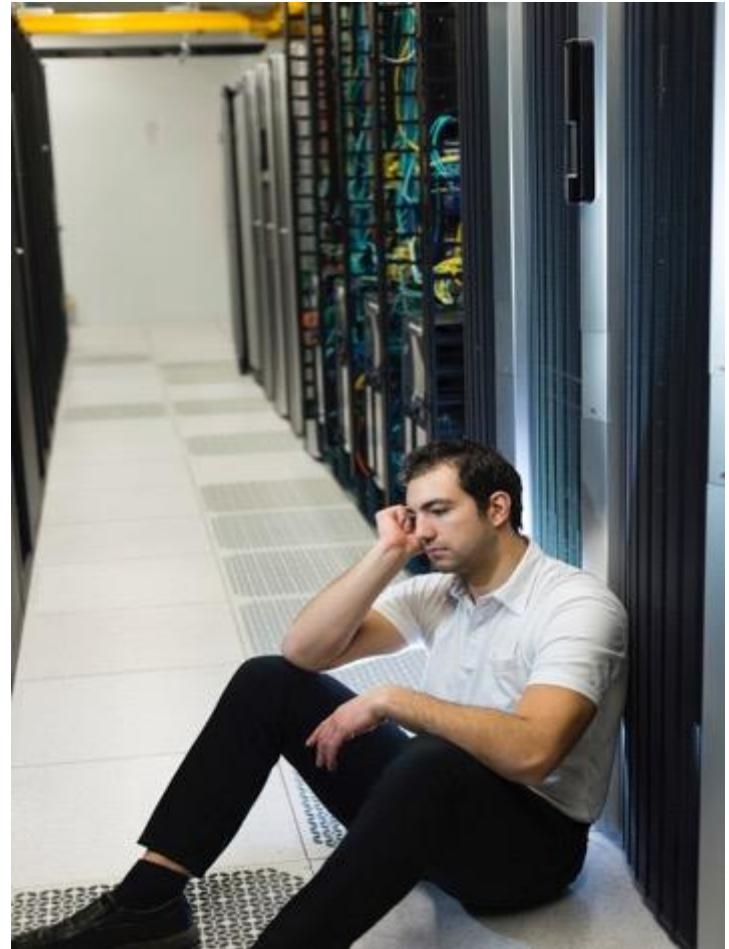
Nation States



# Human Error

Human error is another threat vector

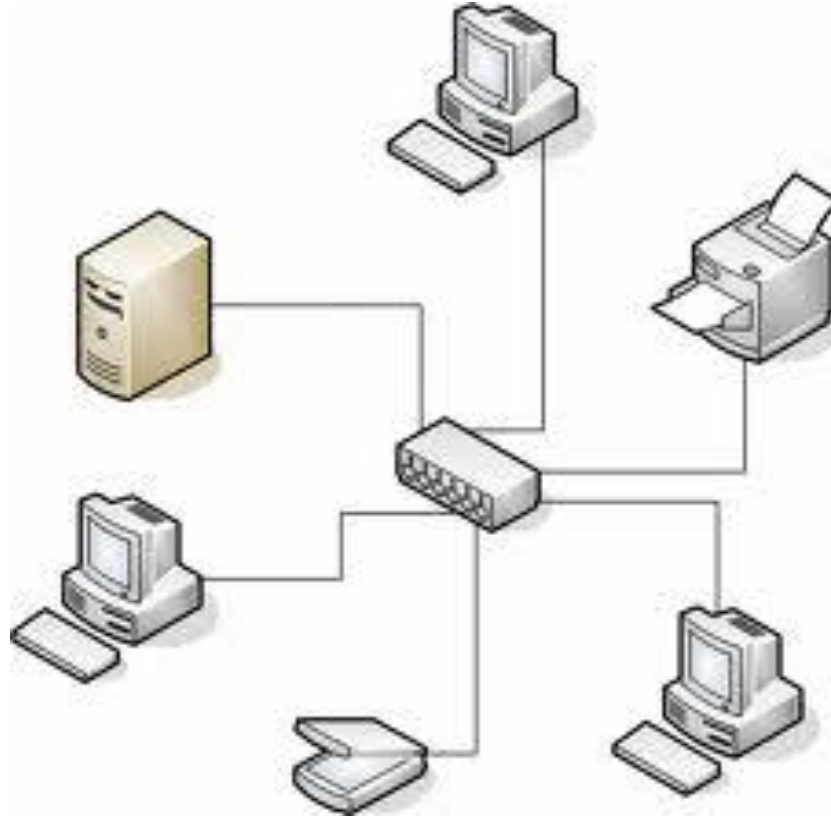
- Poor digital safety practices
- Mistakes in programming (fat finger)
- Other common mistakes



# Vulnerability



# Traditional IT Infrastructure



# The Future Is Here

HEALTH

OCT 4 2016, 11:15 AM ET

---

## **Insulin Pump Vulnerable to Hacking, Johnson & Johnson Warns**

by REUTERS

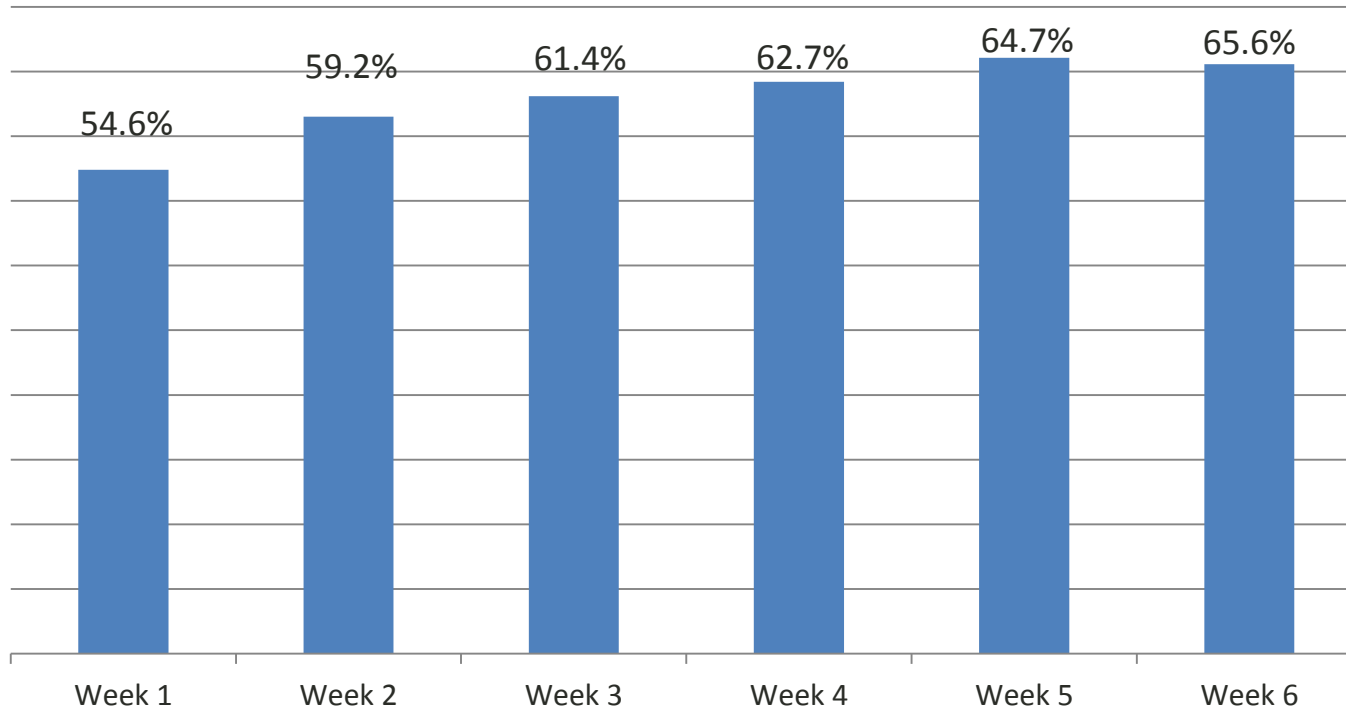
# What Is Our Preparedness Level?

- 75% of organizations are not prepared to respond to cyber attacks
- 55% lack sufficient risk awareness, analysis and assessment
- 32% stated that collaboration between business functions was poor or non-existent, with a direct negative impact on resilience

Yet, 91% said being prepared for an attack is essential to protecting the organization!

# Time-to-Patch

**% of websites owners who fixed a vulnerability after notification**



Cost

# Some Frightening Figures



- The cost of a data breach has gone up 23% since last year
- The cost of each record is \$217
- This includes business interruption costs such as replacing equipment, lack of access to services, and the impact of forensics team has on workflows
- Also includes the compliance costs such as notifying victims (up to \$1 per letter, before the stamp!)

# Montana Breach Costs

- 1.3 million people notified
- Full forensic analysis done
- \$2 million dollar insurance policy utilized for direct costs (such as mailing)
- To date, no one has notified them that their information was used!

# SaudiAramco

- In 2012, malware damaged or destroyed 35,000 computers
- Every office went offline
- Industrial Control Systems were secure but:
  - All payments
  - Invoicing
  - Contracts
  - Communications
  - Had to be done by hand!
- Temporarily adjusted the worldwide price of hard drives up as they rebuilt their infrastructure!



What Are The Events?

# Event Types

- Phishing
- Ransomware
- Lost Devices
- Server Compromise

# Phishing

Dear [REDACTED] customer,

We recently reviewed your account, and suspect that your [REDACTED] Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the [REDACTED] network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your [REDACTED] Internet Banking account. In case you are not enrolled yet for Internet Banking, you will have to use your Social Security Number as both your Personal ID and Password and fill in the required information, including your name and account number.
2. Review your recent account history for any unauthorized withdrawals or deposits, and check your account profile to make sure no changes have been made. If any unauthorized activity has taken place on your account, report to [REDACTED] staff immediately.

To get started, please click the link below:

[https://\[REDACTED\]online.chase.com/colappmgr/XXX](https://[REDACTED]online.chase.com/colappmgr/XXX)

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire [REDACTED] system.

Thank you for your prompt attention to this matter.


Sincerely,


The [REDACTED] BankTeam.


## Wyoming hospital hit by phishing attack

By  
Joseph Goedert

 Print

 Email

 Reprints

 Share

# Ransomware

**BBC** | Sign in | News | Sport | Weather | Shop | Earth | Travel | More

**NEWS**

Home | Video | World | US & Canada | UK | Business | Tech | Science | Magazine | Entertainment

## Technology

### Hollywood hospital held to ransom by hackers



Dave Lee  
North America technology reporter

🕒 15 February 2016 | Technology



Staff at the Hollywood Presbyterian Medical Center are using pen and paper to handle records

HPMC

# Lost/Stolen Devices

- 3,576 Laptops
- **NYC Health Center Notifies 1,500 Patients of**
- **PHI Data Breach**

By [Sara Heath](#) on October 28, 2015

Were left at airports from June 2011 to June 2012

About half were eventually recovered.

The rest were turned over to authorities or donated to charity

# Server Compromise

ADVERTISEMENT

## **Saint Francis Health System server hacked, patient info extracted**

BY JESSICA REMER | MONDAY, SEPTEMBER 19TH 2016

# Special Compliance Costs

- HIPAA
- PCI
- Insurance costs
- HHS OCR:
  - Up to \$1.5 Million for repeating a HIPAA violation
  - OCR also interprets
- Loss of community/patient trust

How Do We Confront The Risk?



# Understand How to Deal with Problems

- Take infected or compromised equipment out of service as soon as practical to prevent further harm
- Notify users as appropriate based on your cyber security policy
- Contact your local law enforcement if you suspect a crime has been committed
- Identify the types of information that you would want to gather during a cyber security incident



# Talk To Your IT Team

It's important to sit down and ask:

- How are we protecting our cyber infrastructure and data?
- What is our plan for responding to a cyber security incident, and what cyber security policies are in place?
- Introduce them Cyber Hygiene, if they are not already familiar...



National Campaign  
for  
**Cyber Hygiene**  
Count, Configure, Control, Patch, Repeat

## 5 Top Priorities

### Count

Know what's connected to and running on your network

### Configure

Implement key security settings to help protect your systems

### Patch

Regularly update all apps, software, and operating systems

### Control

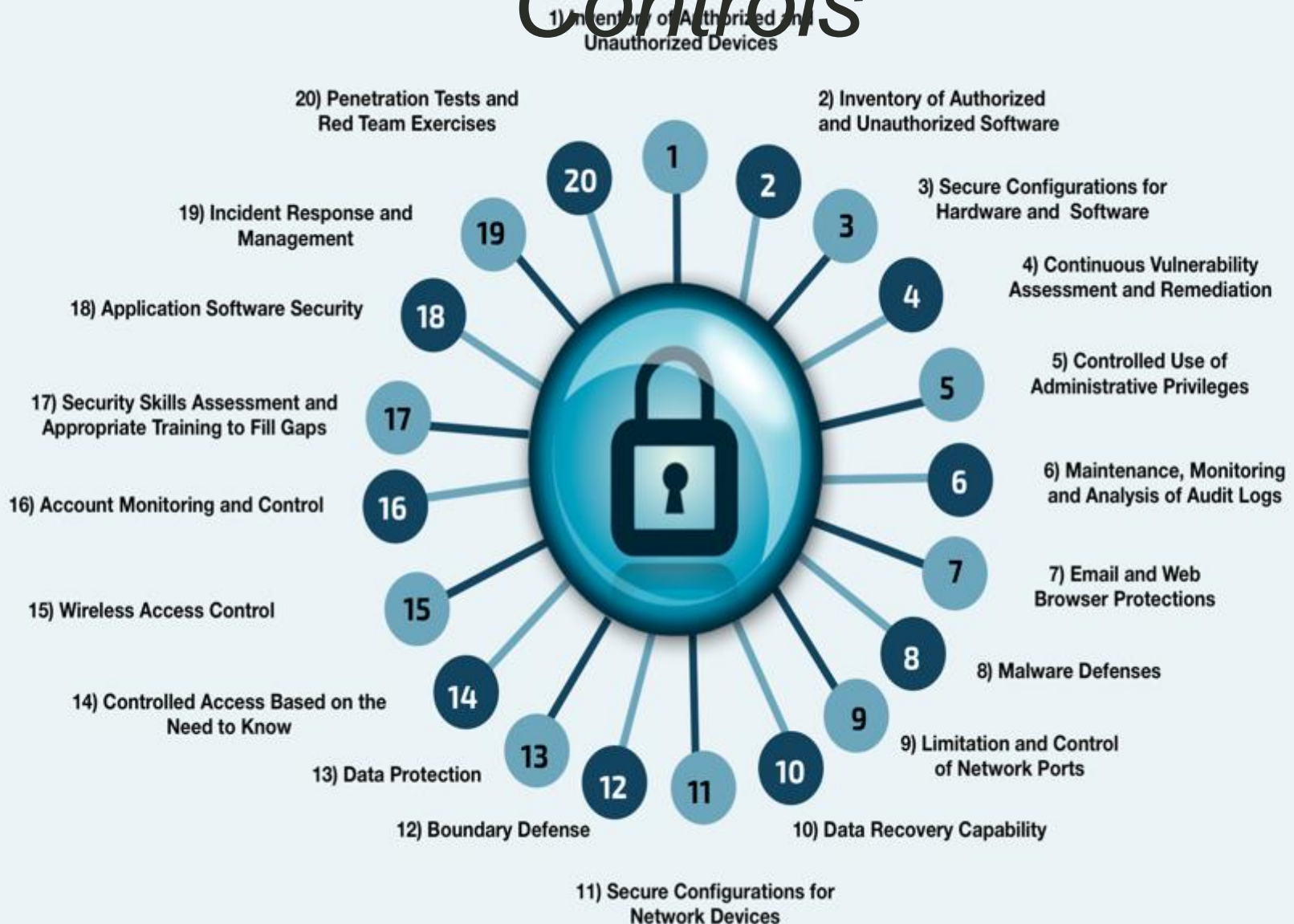
Limit and manage Admin privileges and security settings

### Repeat

Regularize the Top Priorities to form a solid foundation of cybersecurity for your organization. Continue to improve!

# The CIS Critical Security

## Controls



# How Is Cyber Hygiene Like Regular Hygiene?

## Regular Hygiene:

Should be part of our routines

Supported by expert research

Intended to keep us healthy

## Cyber Hygiene:

Should be implemented regularly

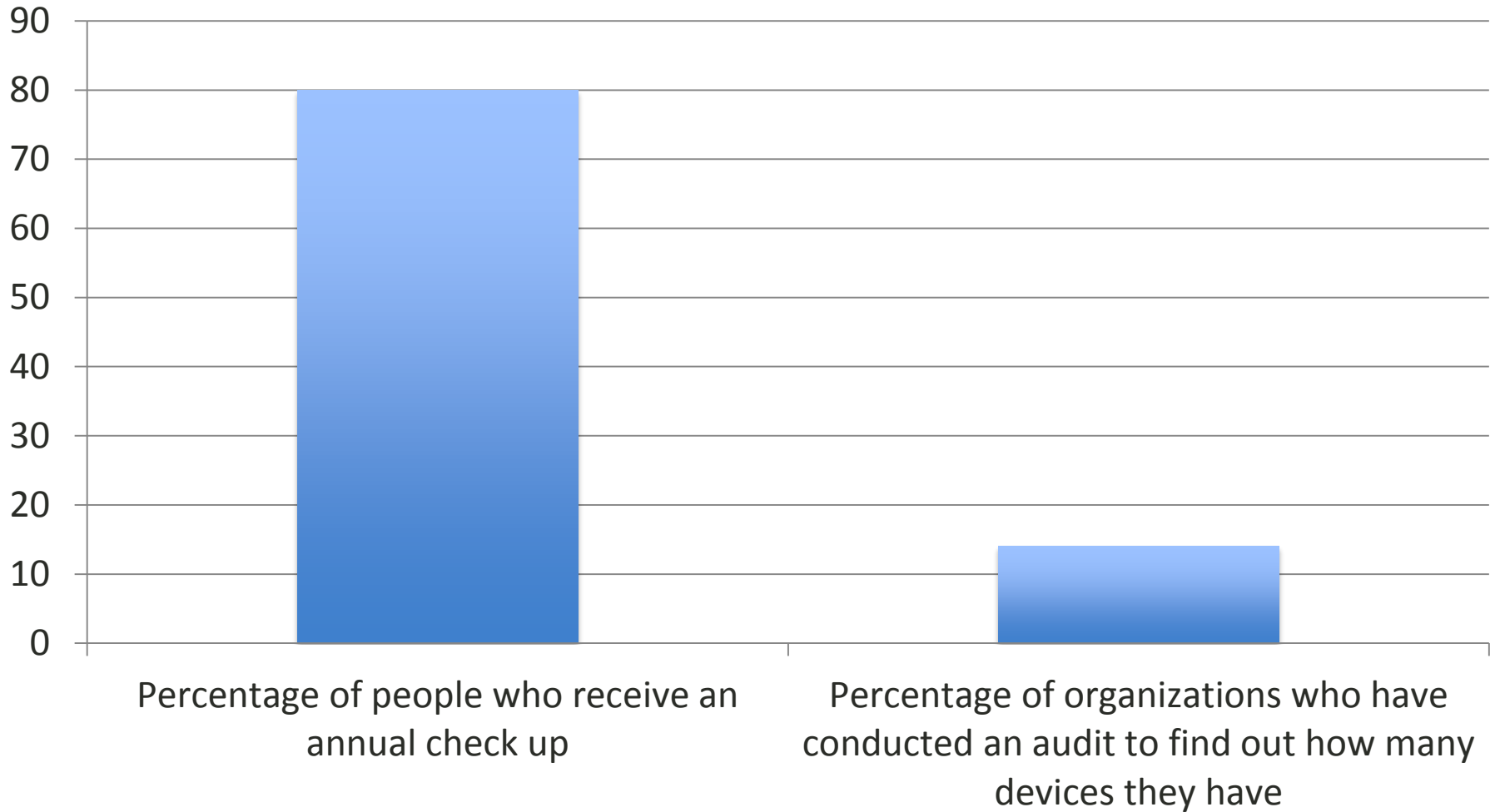
Informed by expert experience

Intended to keep our systems healthy

# Count Hardware (Annual Physical)

- Have your organization check out each device
- Make a list of all assets
  - This list should include:
    - Laptops
    - Desktops
    - Copiers
    - Printers
    - Scanners
    - All equipment that allow information to pass through them and may retain it on their hard drives

## If Organizations Were People Too...



# Count Software (Routine Blood Test)

- You need to know what is running through your “system”
- You need to know what is running through your organizations “systems”, both approved and unapproved
- What should you see?
  - You have an inventory of approved software and the means to identify software on all devices and systems (both approved and unapproved)
  - Prohibiting/blocking end users from installing software is your next step
  - List needs to be monitored, updated and protected!



The business environment has a huge impact on the software you might find!!!!



**“Maybe there’s a reason our blood sugar is up.”**

# Configure (Exercise And Nutrition)

- Security does not just happen, you need to build it through secure configurations
- What are industry-accepted secure configurations/standards?
  - These are recommended standards for securing systems
  - Includes NIST, CIS Benchmarks, others
  - Covers items like password length, encryption, and port access

# Configure (Exercise And Nutrition)

- Why is this critical:
  - These configuration standards have been thoroughly tested with security in mind. Most software and hardware out of the box is only partially securely configured
  - You aren't born fit... you have to work at it!
- What does it look like
  - You have a standardized hardened image
  - Follow strict configuration management (change control board)

# Why Is This Hard?



We need all configuration changes reviewed by the change control board and signed off by a senior exec



We can make any change our users need to configurations, especially if its really important for them to fulfill their

# Patch (Vaccination)

- Like vaccines for polio, measles, and tetanus, there are vaccines for your computer against known attacks
- Why is this critical:
  - Unpatched systems are one of the primary ways attackers gain access. A good patching practice reduces the risk of exploitation
- It is important to patch all applications and on a regular basis

# Control Passwords (Wash Your Hands)

- Do you wash your hands regularly (with soap)?
- Do you require users to have complex password?
- What is a complex password?
  - A password that has the following:
    - At least 10 characters
    - Uppercase, lowercase, numbers and symbols
    - No words or proper names
    - No personal information

# Human Error example– bad passwords!

## Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17512

tomshard.com

# Control (Stay Home)

- Do you advise employees to stay home when they are sick?
- Do you limit the number of users with administrative privileges?
- Why is this critical:
  - When administrative privileges are keys to the kingdom
  - If an admin gets “infected” it’s a **big** problem
- What does it look like:
  - No end users with administrative
  - Ideally limiting it to just the Network and/or System Administrators (and it is validated!!!!)



# What else can you do?

- CIS can provide alerts and warnings on cyber threats and free resources on best practices and awareness tools
- The CIS Critical Security Controls and CIS Security Benchmarks are both free to download
- CIS offers additional services to further strengthen cyber posture:
  - Consulting
  - White papers
  - Other resources

# Other Great Resources

- US-CERT - [www.us-cert.gov/](http://www.us-cert.gov/)
- Internet Crime Complaint Center [www.ic3.gov/](http://www.ic3.gov/)
- National Cyber Security Alliance:  
[www.staysafeonline.org](http://www.staysafeonline.org)

Thank You!

Questions???????

Contact Information

[ryan.spelman@cisecurity.org](mailto:ryan.spelman@cisecurity.org)

518-880-0699

[www.cisecurity.org](http://www.cisecurity.org)