Digital Healthcare

Yordan Iliev
Director R&D
Healthcare

Regional Cybersecurity Forum, 29-30 November 2016, Grand Hotel Sofia, Bulgaria

sqilline
brilliant beyond borders

AGENDA

Introduction

Security challenges in healthcare IT

Change ahead

Conclusions, Recommendations & Experience

Q&A

- Sqilline –
Quick Facts

SAP Partner

Sqilline- SAP Mobility Partner leading in CEE

- SAP Application Development Partner for Innovation Packs

Established

- 2009

Competence Center SAP Mobility

- Sofia, Bulgaria

Focus

- Delivering innovation technology in healthcare

Team

25 + SAP mobile developers and architectures

sqilline
brilliant beyond borders

Your trusted SAP Mobility partner

Sqilline services

Providing Analytic Healthcare solutions – based on SAP Hana database technology. The solutions are integrated to any HIS/ HL7 CDA.

Development of customer made mobile solutions - develop hybrid and native mobile application based on SAP Mobile Platform and SAP Hana Cloud Platform.

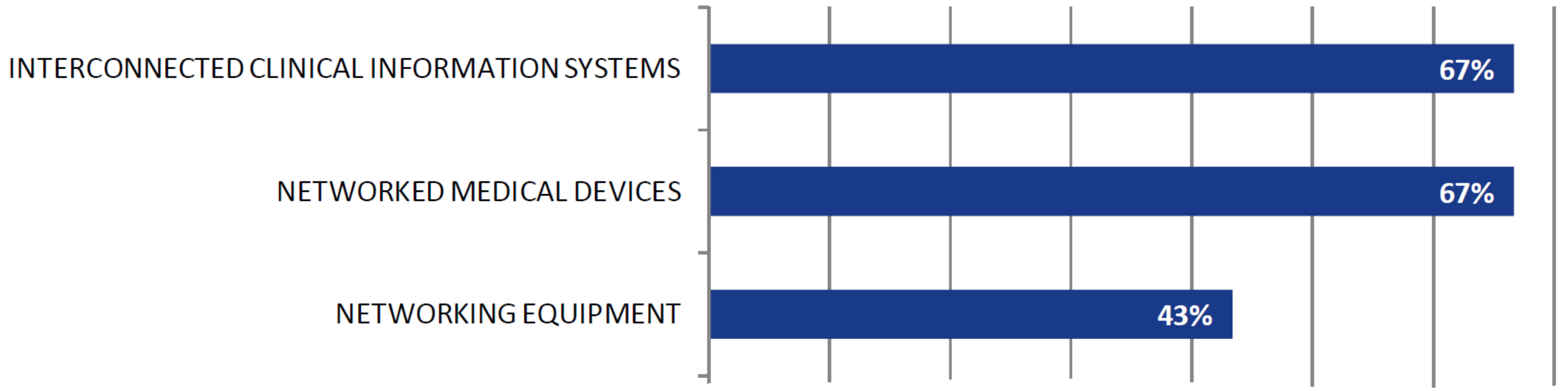
SAP ERP Implementation& Maintenance services – with more than 10 years experience, Sqilline implements and support SAP ERP system.

SMART HOSPITAL

“Hospital, that relies on optimized and automated processes built on ICT environment of interconnected assets, particularly based on Internet of Things (IoT), to improve existing patient care procedures and introduce new capabilities”

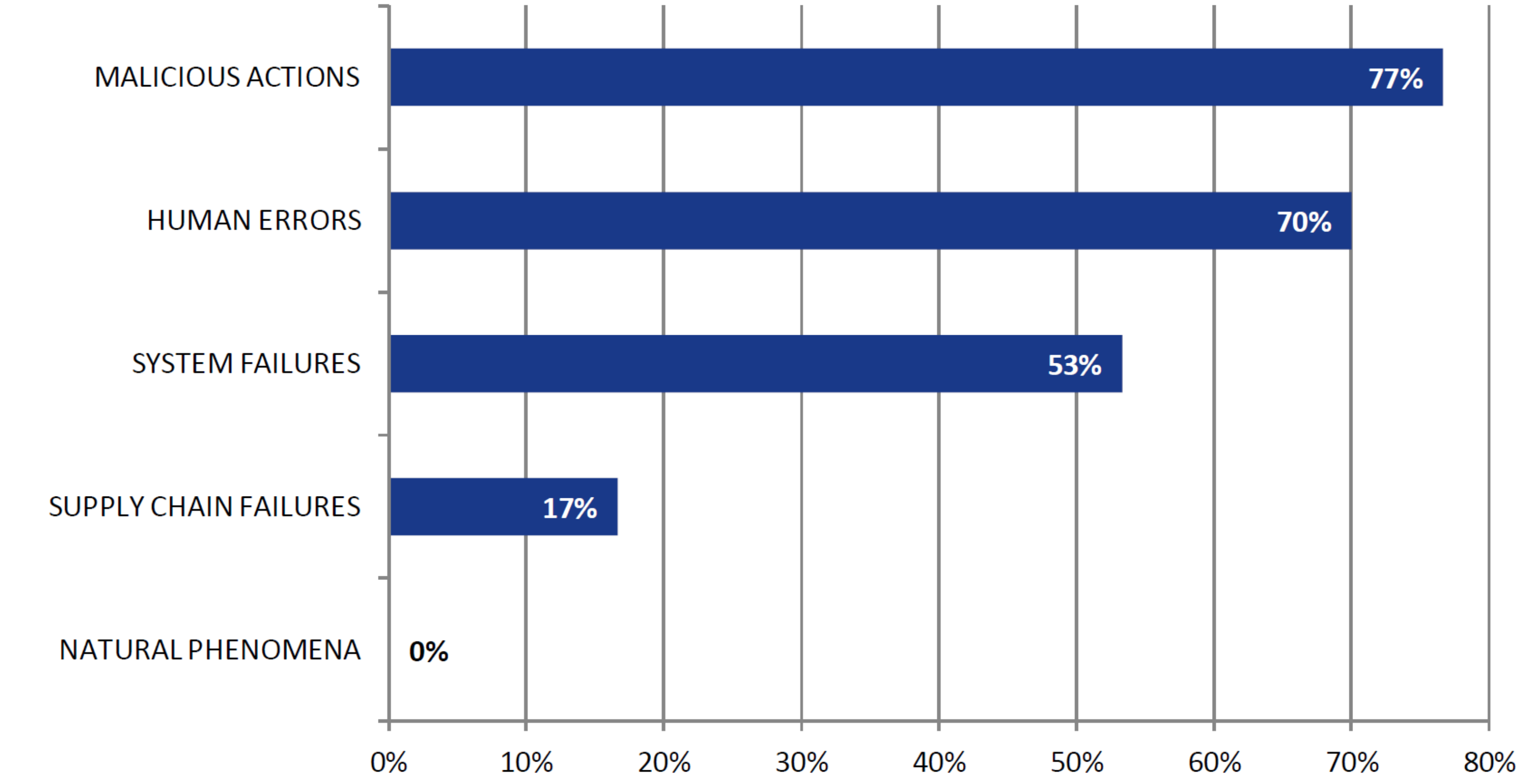
Source: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Smart hospitals most critical infrastructure



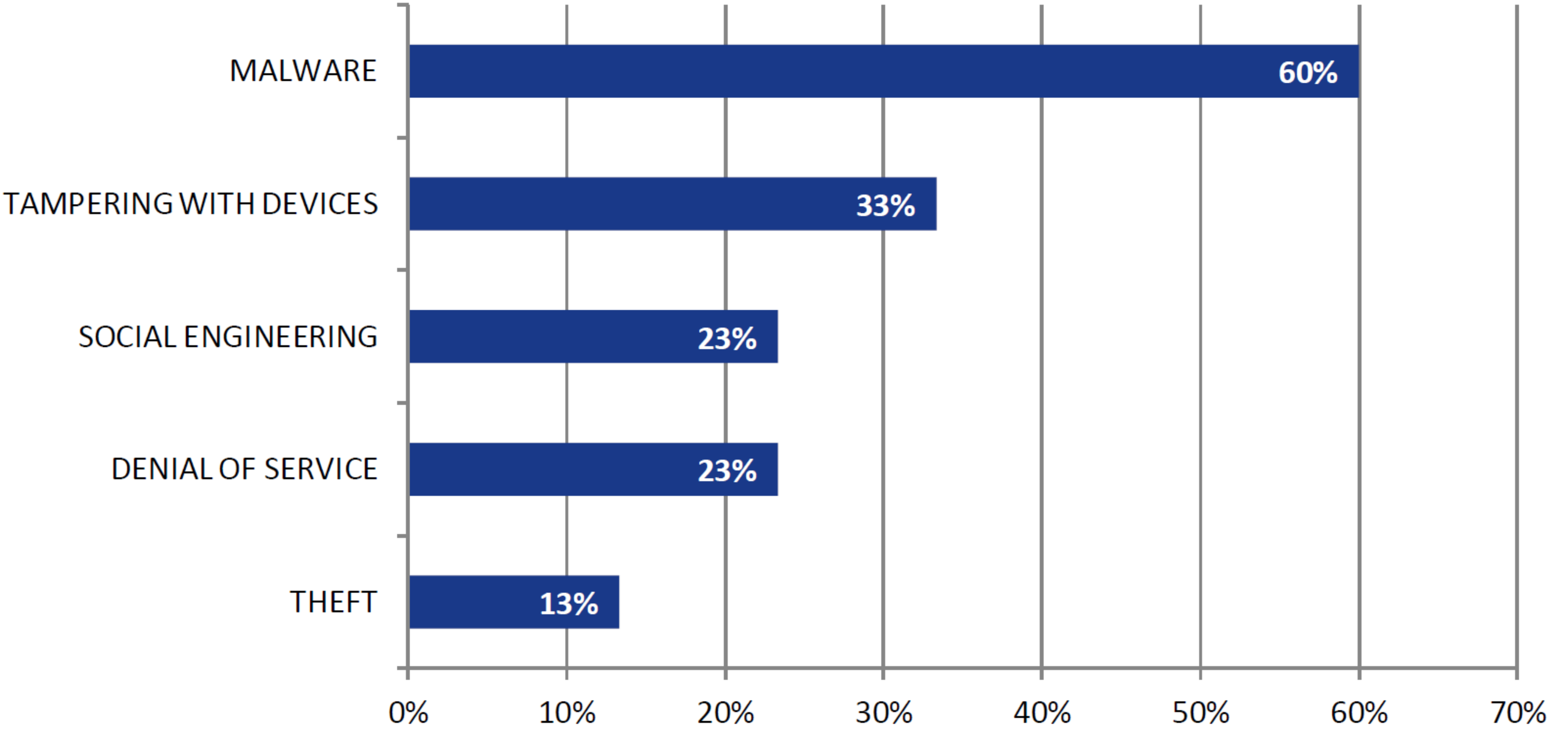
Source: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Critical threats for smart hospital



Source: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Common attack scenarios for smart hospitals



Source: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

California Hospital Pays $17,000 To Hackers In ‘Ransomware’ Attack

February 18, 2016 9:58 AM

Filed Under: Hackers, Hollywood Presbyterian Medical Center, Hospital, Ransomware

Privacy & Security

Two more hospitals struck by ransomware, in California and Indiana

Both Alvarado Hospital Medical Center and King's Daughters' Health say that quick response times appear to have minimized potential damage.

By Mike Miliard | April 04, 2016 | 10:55 AM

NEWS

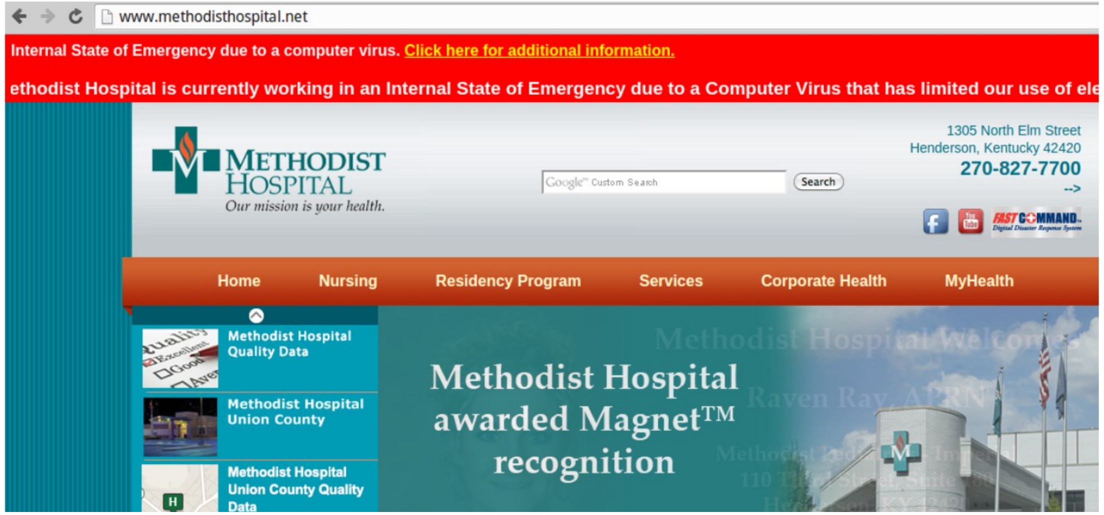
Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers

Network has been offline fore more than a week, $3.6 million demanded as ransom

22
MAR 16

Hospital Declares ‘Internal State of Emergency’ After Ransomware Infection

A Kentucky hospital says it is operating in an “internal state of emergency” after a ransomware attack rattled around inside its networks, encrypting files on computer systems and holding the data on them hostage unless and until the hospital pays up.



www.methodisthospital.net

Internal State of Emergency due to a computer virus. Click here for additional information.

ethodist Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of ele

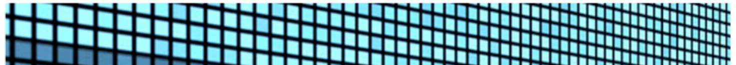
METHODIST HOSPITAL
Our mission is your health.
Google™ Custom Search
Search
1305 North Elm Street
Henderson, Kentucky 42420
270-827-7700
-->
FAST COMMAND
Digital Disaster Response System
Home
Nursing
Residency Program
Services
Corporate Health
MyHealth
Methodist Hospital Quality Data
Methodist Hospital Union County
Methodist Hospital Union County Quality Data
Methodist Hospital awarded Magnet™ recognition
Methodist Hospital Welcomes
Raven Ray, APRN

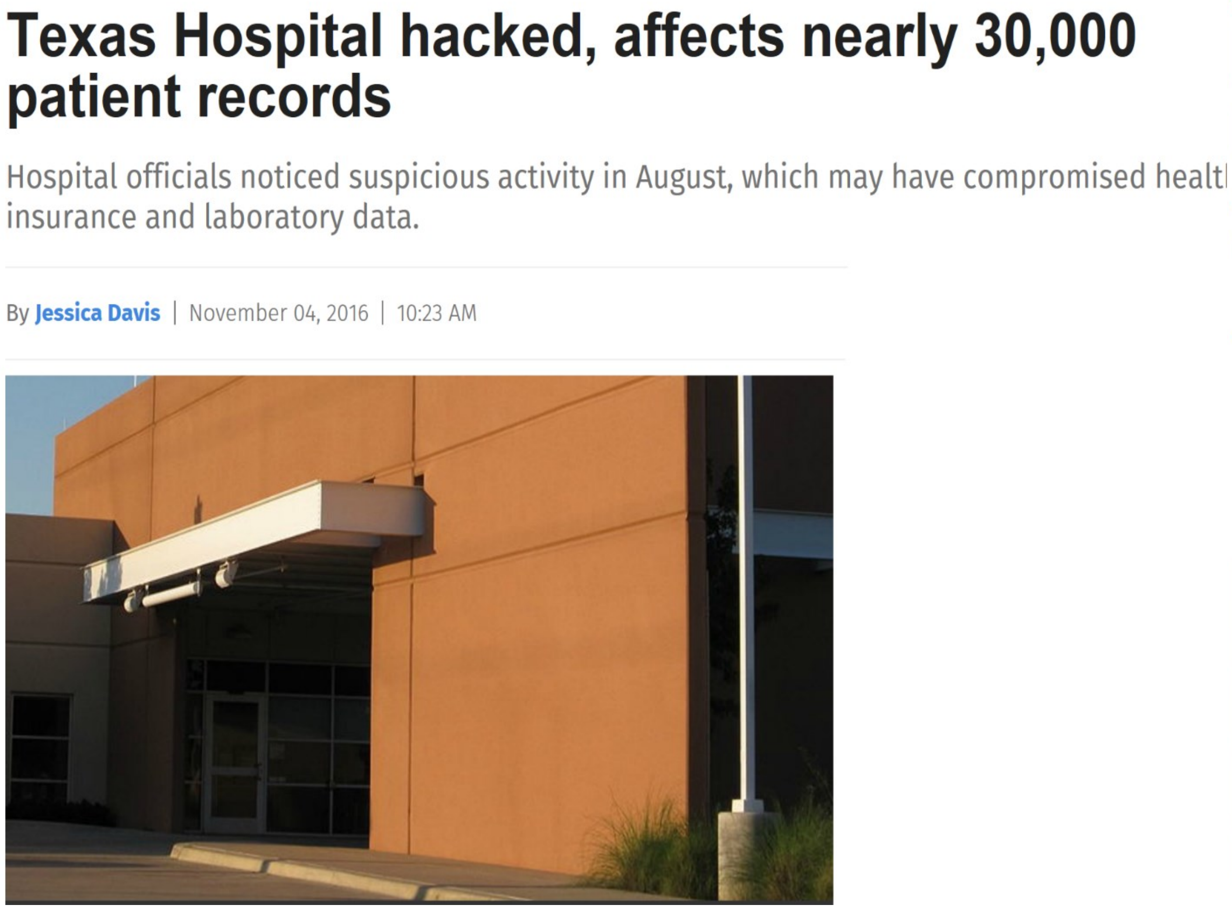
Privacy & Security

Ransomware: 97 percent of phishing e-mails contain it

Locky dominates the onslaught. And there has been an increase in deployment of so-called quiet malware such as remote access Trojan malware like jRAT, according to new research from PhishMe.

By Bill Siwicki | November 18, 2016 | 08:44 AM

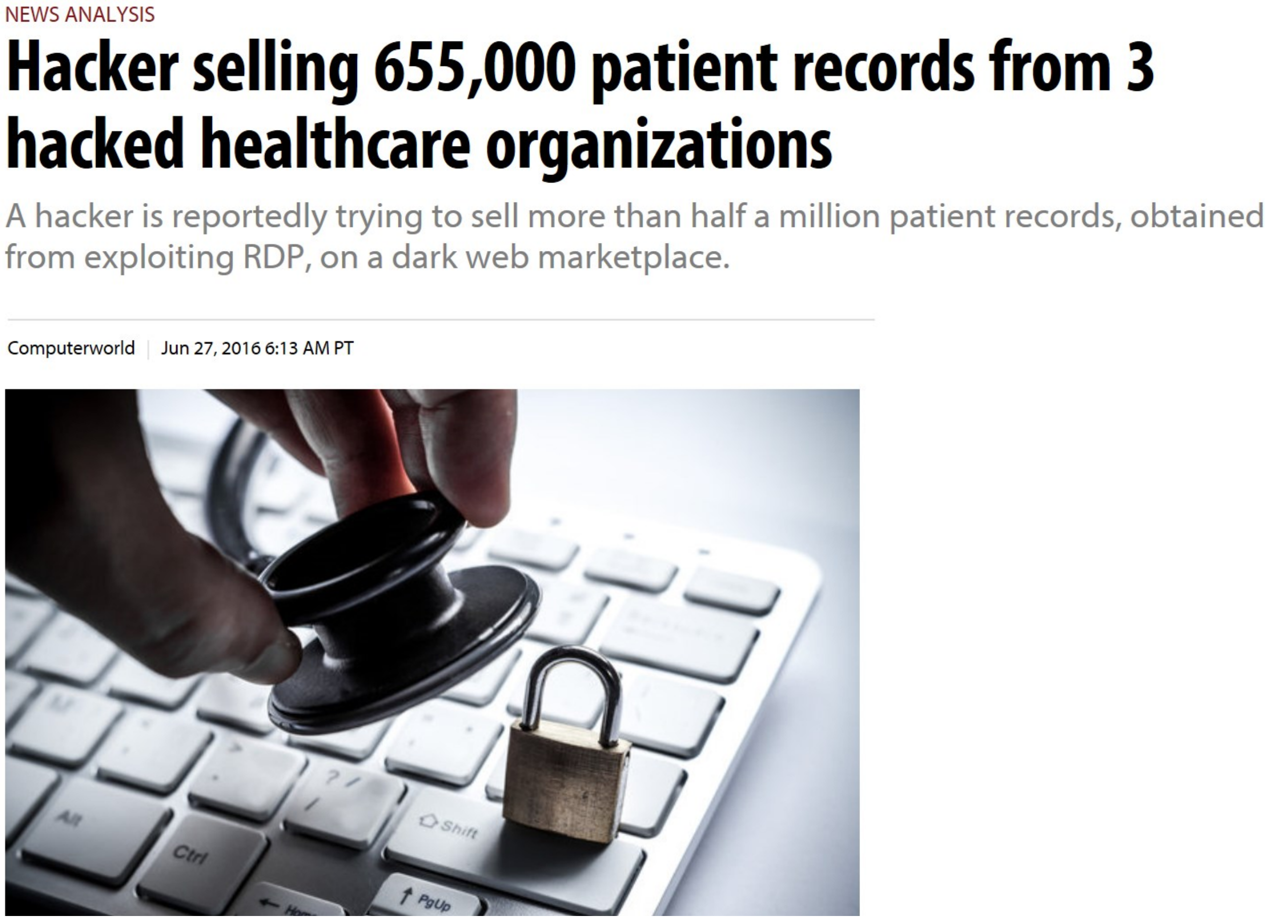




Texas Hospital hacked, affects nearly 30,000 patient records

Hospital officials noticed suspicious activity in August, which may have compromised healt insurance and laboratory data.

By Jessica Davis | November 04, 2016 | 10:23 AM

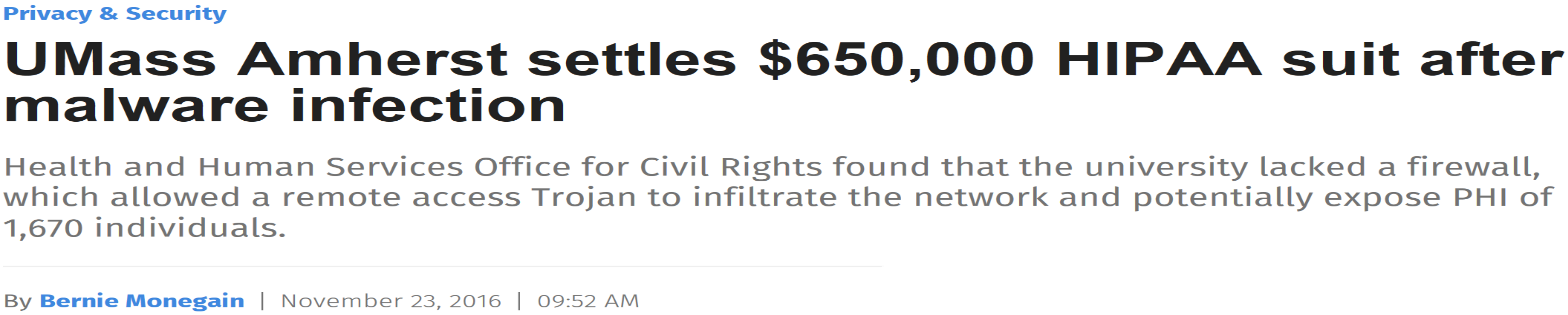


NEWS ANALYSIS

Hacker selling 655,000 patient records from 3 hacked healthcare organizations

A hacker is reportedly trying to sell more than half a million patient records, obtained from exploiting RDP, on a dark web marketplace.

Computerworld | Jun 27, 2016 6:13 AM PT

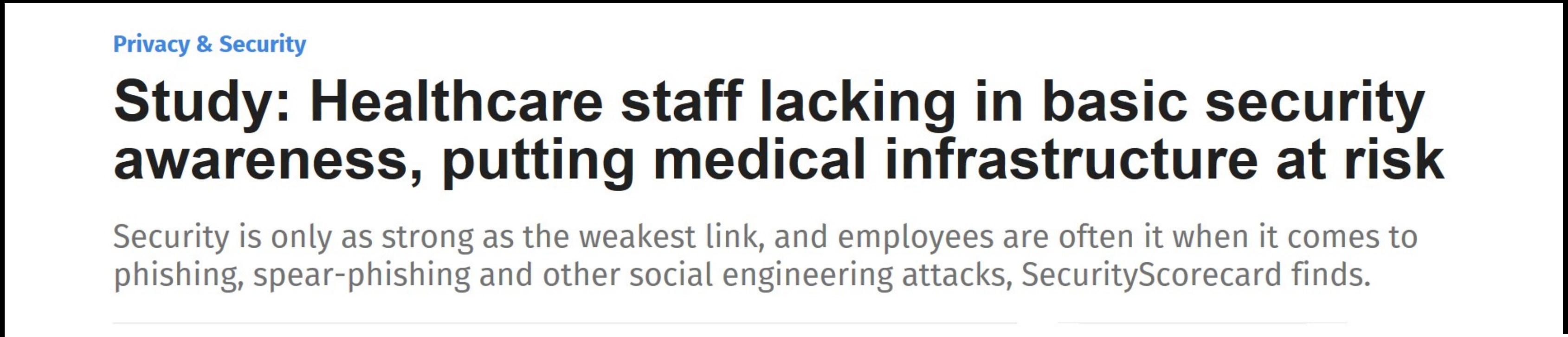


Privacy & Security

UMass Amherst settles $650,000 HIPAA suit after malware infection

Health and Human Services Office for Civil Rights found that the university lacked a firewall, which allowed a remote access Trojan to infiltrate the network and potentially expose PHI of 1,670 individuals.

By Bernie Monegain | November 23, 2016 | 09:52 AM

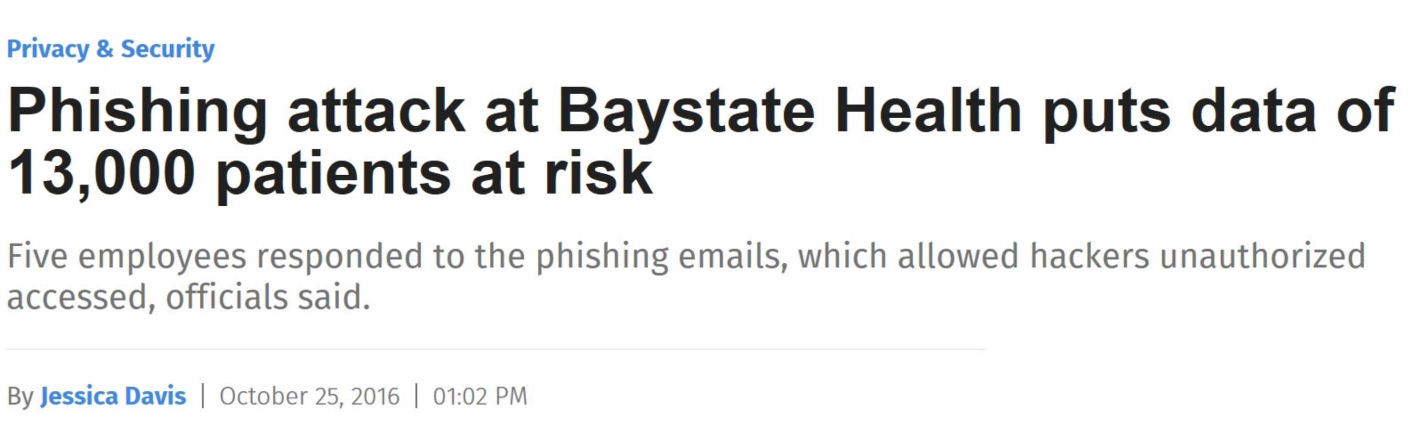


Privacy & Security

Study: Healthcare staff lacking in basic security awareness, putting medical infrastructure at risk

Security is only as strong as the weakest link, and employees are often it when it comes to phishing, spear-phishing and other social engineering attacks, SecurityScorecard finds.

By Bill Siwicki | October 27, 2016 | 09:27 AM

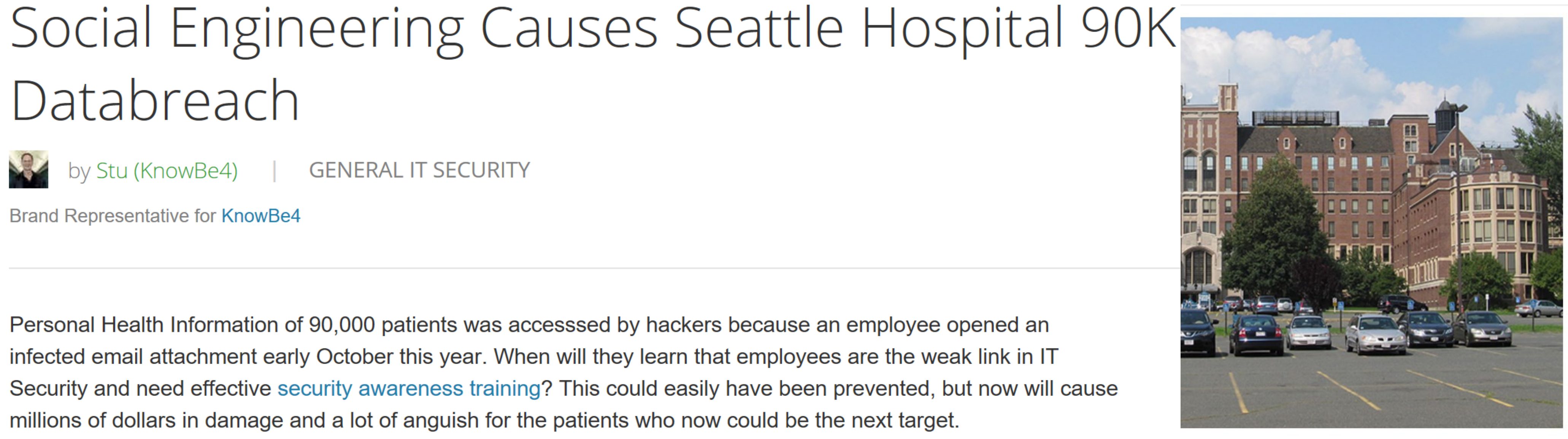


Privacy & Security

Phishing attack at Baystate Health puts data of 13,000 patients at risk

Five employees responded to the phishing emails, which allowed hackers unauthorized accessed, officials said.

By Jessica Davis | October 25, 2016 | 01:02 PM



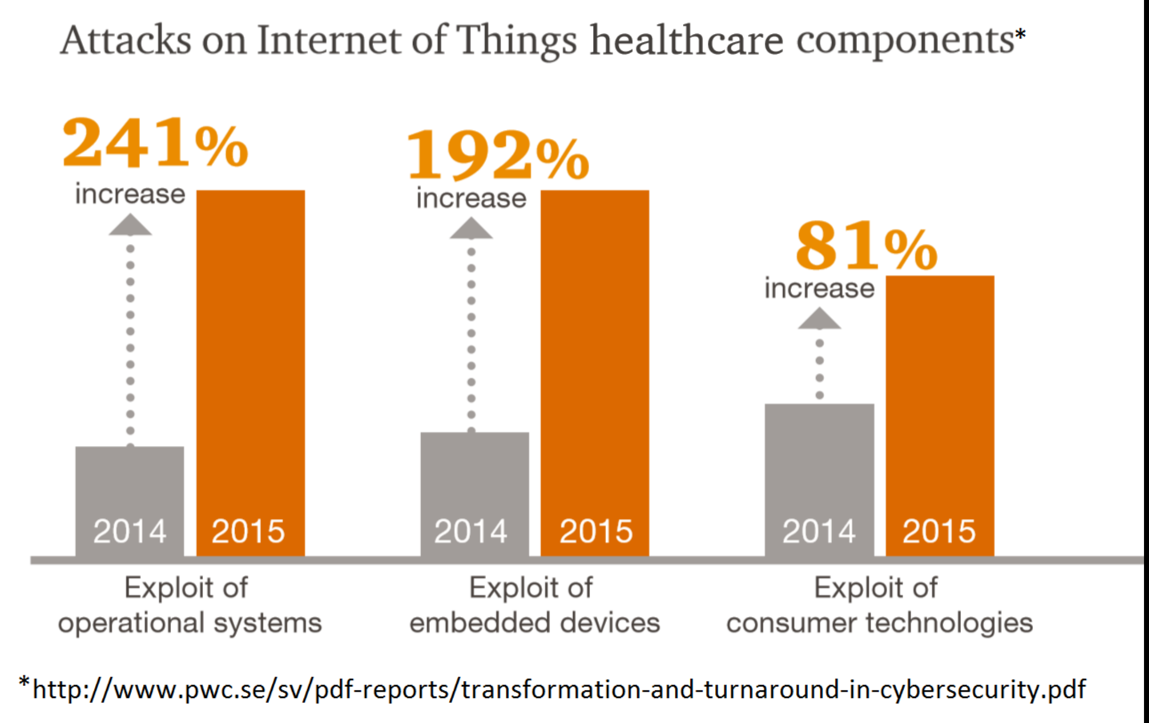
Social Engineering Causes Seattle Hospital 90K Databreach

by Stu (KnowBe4) | GENERAL IT SECURITY

Brand Representative for KnowBe4

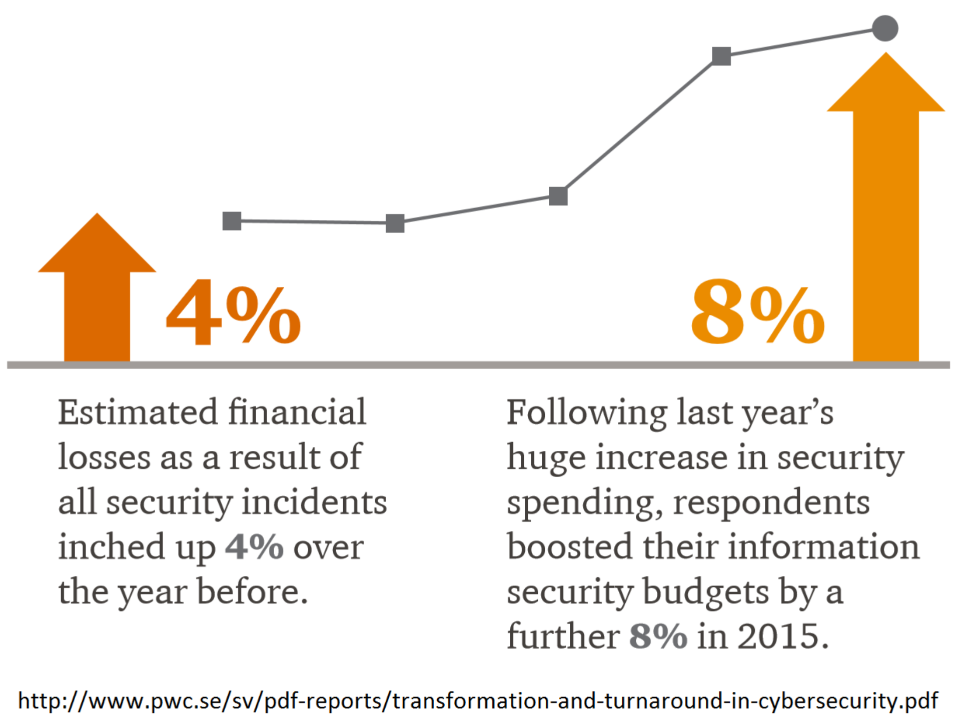
Personal Health Information of 90,000 patients was accesssed by hackers because an employee opened an infected email attachment early October this year. When will they learn that employees are the weak link in IT Security and need effective security awareness training? This could easily have been prevented, but now will cause millions of dollars in damage and a lot of anguish for the patients who now could be the next target.

Internet of Things? Internet of Threats? or Internet of Trouble?



Attacks on Internet of Things healthcare components*

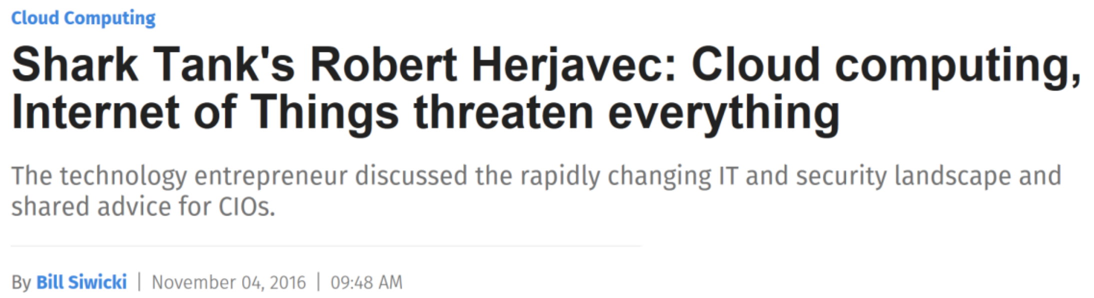
*http://www.pwc.se/sv/pdf-reports/transformation-and-turnaround-in-cybersecurity.pdf



Estimated financial losses as a result of all security incidents inched up **4%** over the year before.

Following last year's huge increase in security spending, respondents boosted their information security budgets by a further **8%** in 2015.

http://www.pwc.se/sv/pdf-reports/transformation-and-turnaround-in-cybersecurity.pdf

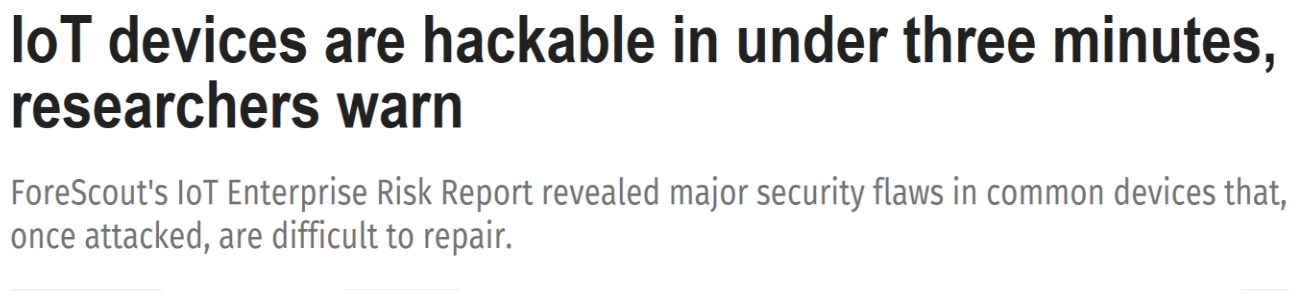


Cloud Computing

Shark Tank's Robert Herjavec: Cloud computing, Internet of Things threaten everything

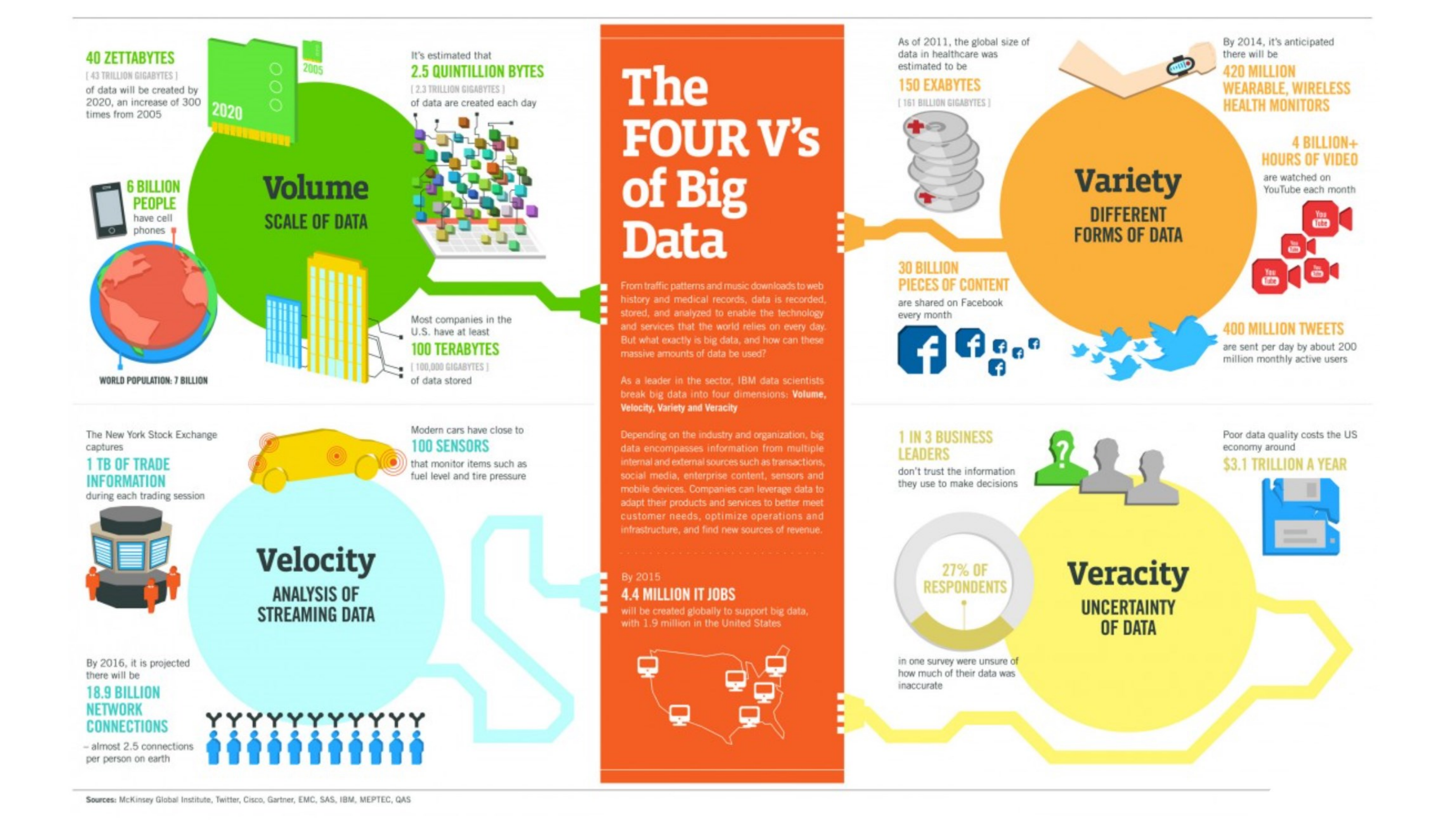
The technology entrepreneur discussed the rapidly changing IT and security landscape and shared advice for CIOs.

By Bill Siwicki | November 04, 2016 | 09:48 AM



IoT devices are hackable in under three minutes, researchers warn

ForeScout's IoT Enterprise Risk Report revealed major security flaws in common devices that, once attacked, are difficult to repair.



The FOUR V's of Big Data

From traffic patterns and music downloads to web history and medical records, data is recorded, stored, and analyzed to enable the technology and services that the world relies on every day. But what exactly is big data, and how can these massive amounts of data be used?

As a leader in the sector, IBM data scientists break big data into four dimensions: **Volume, Velocity, Variety and Veracity**

Depending on the industry and organization, big data encompasses information from multiple internal and external sources such as transactions, social media, enterprise content, sensors and mobile devices. Companies can leverage data to adapt their products and services to better meet customer needs, optimize operations and infrastructure, and find new sources of revenue.

By 2015
4.4 MILLION IT JOBS
will be created globally to support big data, with 1.9 million in the United States

Volume

SCALE OF DATA

40 ZETTABYTES
[43 TRILLION GIGABYTES]
of data will be created by 2020, an increase of 300 times from 2005

It's estimated that
2.5 QUINTILLION BYTES
[2.3 TRILLION GIGABYTES]
of data are created each day

6 BILLION PEOPLE
have cell phones

WORLD POPULATION: 7 BILLION

Most companies in the U.S. have at least
100 TERABYTES
[100,000 GIGABYTES]
of data stored

Variety

DIFFERENT FORMS OF DATA

As of 2011, the global size of data in healthcare was estimated to be
150 EXABYTES
[161 BILLION GIGABYTES]

By 2014, it's anticipated there will be
420 MILLION WEARABLE, WIRELESS HEALTH MONITORS

4 BILLION+ HOURS OF VIDEO
are watched on YouTube each month

30 BILLION PIECES OF CONTENT
are shared on Facebook every month

400 MILLION TWEETS
are sent per day by about 200 million monthly active users

Velocity

ANALYSIS OF STREAMING DATA

The New York Stock Exchange captures
1 TB OF TRADE INFORMATION
during each trading session

Modern cars have close to
100 SENSORS
that monitor items such as fuel level and tire pressure

By 2016, it is projected there will be
18.9 BILLION NETWORK CONNECTIONS
– almost 2.5 connections per person on earth

Veracity

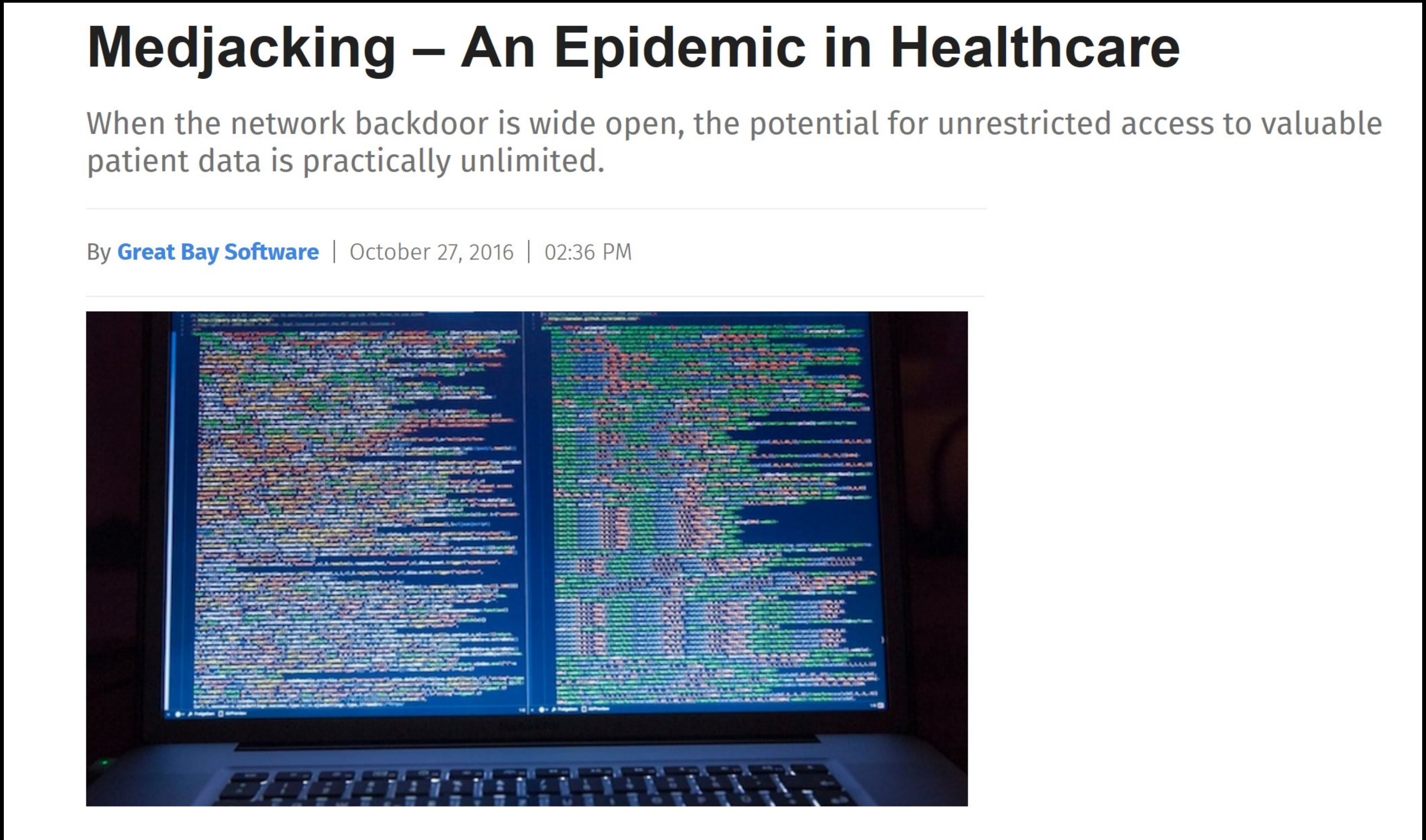
UNCERTAINTY OF DATA

1 IN 3 BUSINESS LEADERS
don't trust the information they use to make decisions

Poor data quality costs the US economy around
$3.1 TRILLION A YEAR

27% OF RESPONDENTS
in one survey were unsure of how much of their data was inaccurate

Sources: McKinsey Global Institute, Twitter, Cisco, Gartner, EMC, SAS, IBM, MEPTEC, QAS

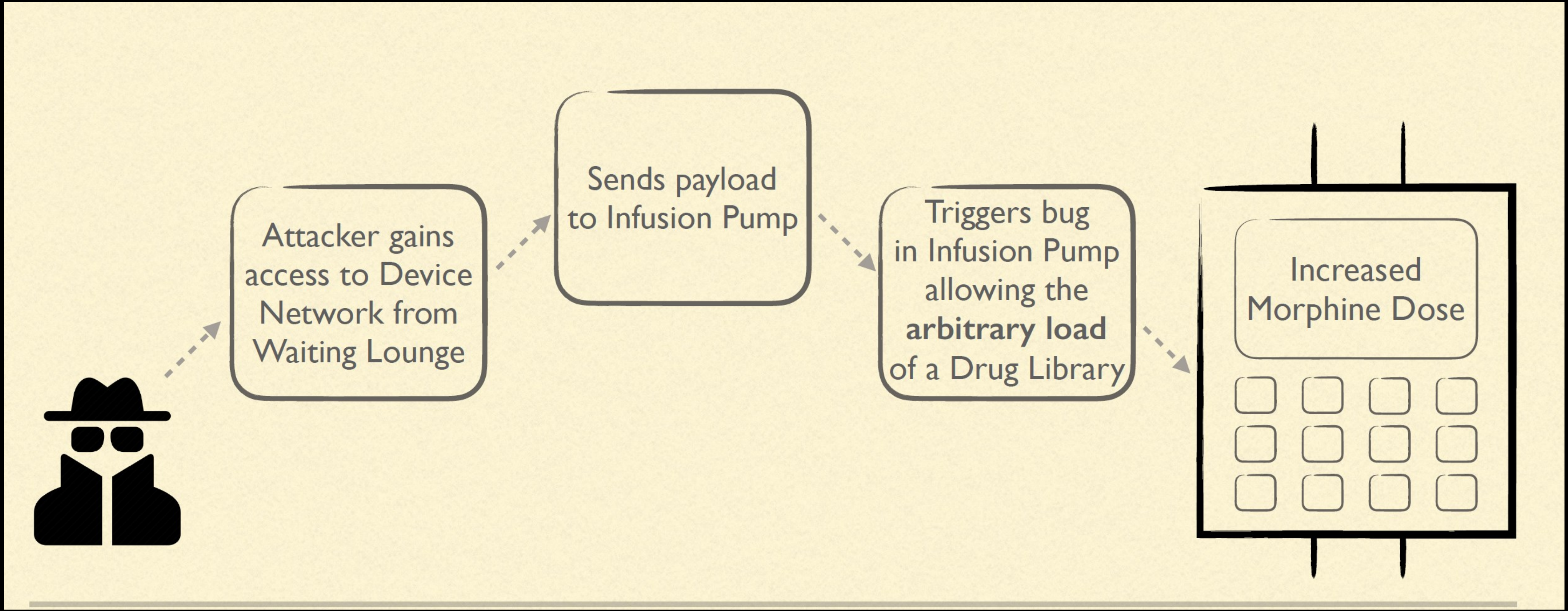


Medjacking – An Epidemic in Healthcare

When the network backdoor is wide open, the potential for unrestricted access to valuable patient data is practically unlimited.

By **Great Bay Software** | October 27, 2016 | 02:36 PM

Example attack scenario



Attacker gains access to Device Network from Waiting Lounge
Sends payload to Infusion Pump
Triggers bug in Infusion Pump allowing the **arbitrary load** of a Drug Library
Increased Morphine Dose

Source: https://census-labs.com

Key findings of 2016 annual HC industry cybersecurity report

- Over 75% of the entire healthcare industry has been infected with malware over the last year
- 88% of all healthcare manufacturers have had malware infections.
- 96% of all ransomware affecting the healthcare industry targeted medical treatment centers.
- Healthcare is 5th highest in ransomware counts among all industries.
- 40% of breached companies had a C or Lower in Network Security at the time of breach.
- Over 50% of the healthcare industry has a Network Security score of a C or Lower.
- 63% of the 27 Biggest US Hospitals have a score of C or lower in Patching Cadence

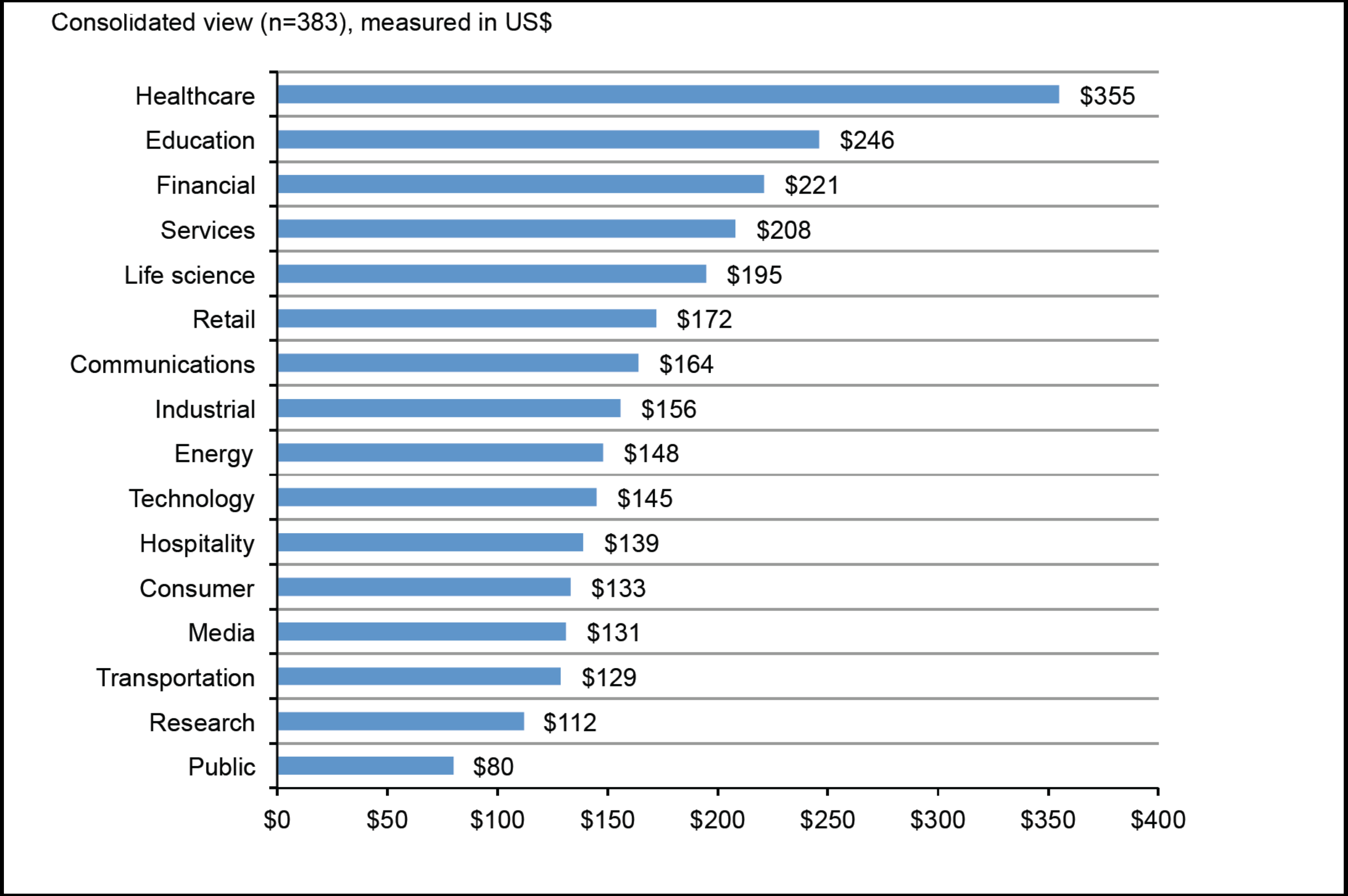
Source: https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Healthcare_Report_Final.pdf

Cost of data Breach in 2016

- $4 million is the average total cost of data breach
- 29% increase in total cost of data breach since 2013
- 15% increase per capita cost since 2013
- $158 average cost per lost or stolen record in all industries
- **$355** average cost per lost or stolen record in healthcare organizations

Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Per capita cost by industry classification



Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Common factors for most incidents

- Misunderstanding its compliance scope
- Compliance before security
- The organization doesn’t conduct risk assessments
- Not considering best practices
- Using an insecure providers
- Lack of awareness, knowledge or attention

A SHIP IS SAFE IN HARBOR BUT …

THAT'S NOT WHAT SHIPS ARE BUILT FOR.

- John A. Shedd

Photo © the_tahoe_guy (Flickr)

CHANGE
AHEAD

Top 5 ways cloud computing making IT inroads

1. Data security: resiliency
2. Data security: privacy
3. Speed of innovation
4. Mobile applications
5. Developing trends

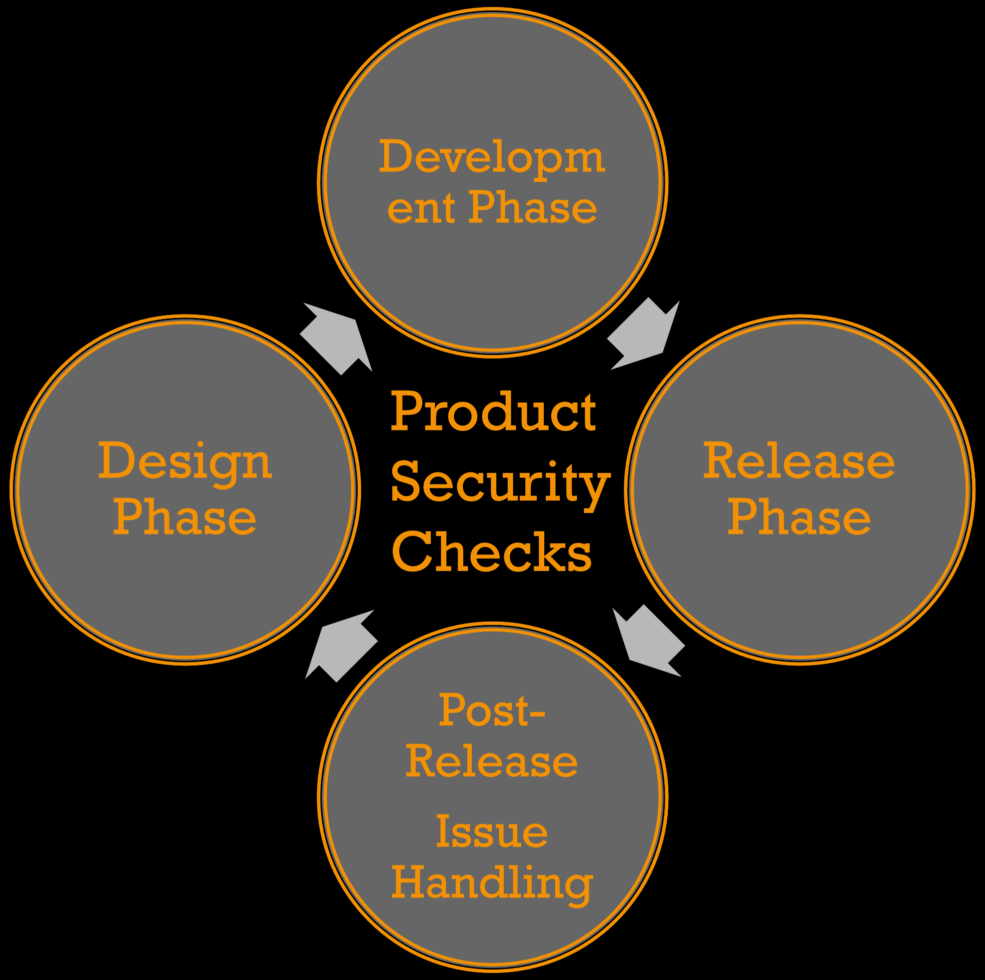
The way forward …

Security Architecture for Medical Devices setups:

1. **Control** physical, network and service access;
2. **Audit** interactions (tie to per-user accounts, no common / default credentials;
3. **Protect** data storage and transmission

The way forward …

Medical Devices need to pass three levels of Security Assessments prior to use



Development Phase

Release Phase

Post-Release Issue Handling

Design Phase

Product Security Checks

Secure SDLC followed by Vendor

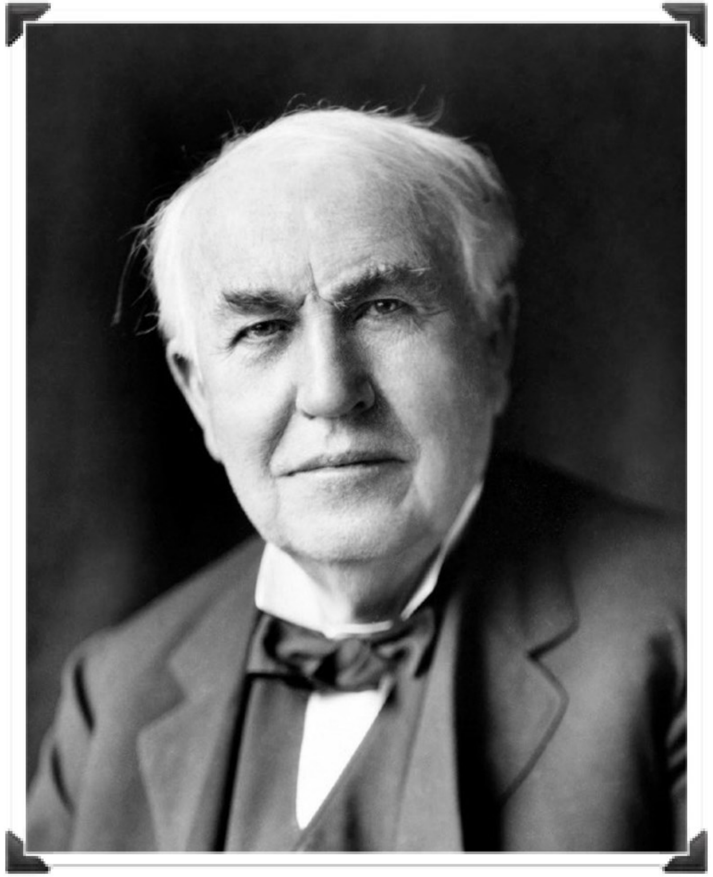
Model Security Assessment

Independent Assessment executed / commissioned by Certification Body

Setup Security Assessment

Independent Assessment executed / commissioned by Medical Institution

A holistic vision



Rectangular Snip

Thomas Edison, 1847-1931

‘A vision without execution is a hallucination’

Recommendations for executions

1. Identification of critical eHealth infrastructure and definition of levels
2. Cybersecurity guidelines
3. Cost benefit analysis of the security incidents
4. eHealth incident reporting system
5. Information sharing and interchange
6. Baseline security measures
7. Implementations of widely accepted security standards
8. Raise awareness and knowledge of cybersecurity
9. eHealth cybersecurity strategy should be aligned nationally

EU Experience

1. Finalnd – The ESKO project:
   - Own EHR nationwide
   - Own private cloud since 1996
   - Cloud service for regional professionals
   - 5G in progress …
2. Austria – The ELGA project:
   - 3 stakeholders – government, HIFs, all the 8 regions
   - Implementing IHE standard for security compliance and regulations, exchange & interoperability of patient information
   - Officially started in 2007

EU Experience

3. Norway – eHealth national priority
    - Own secure telecommunications network developed and managed by the government
    - Provide efficient and secure electronic exchange of patient information between all relevant parties within the health and social services sector
    - Most healthcare organizations are connected
    - 700 000 electronic messages sent through the health network every day
    - Code of conduct – end to
    - HealthCERT – shares knowledge about ICT threats and protection mechanisms and continuously monitors traffic within the health network
    - National protection program
4. EU commission
    - The JAseHN (http://jasehn.eu/)
    - eHealth Digital Service Infrastructure (http://ec.europa.eu/health/ehealth/policy/network/index_en.htm)

Q&A

Yordan Iliev

Director

Research & Development

Healthcare

M: Yordan.iliev (at) Sqilline.com

W: sqilline.com

sqilline

brilliant beyond borders