eHI
eHEALTH INITIATIVE

2018 Guide to Building Your Security Strategy

January 23, 2018
1 pm – 2 pm ET

Agenda

- Welcome and Introductions
  - Claudia Ellison, Program Director, eHealth Initiative
- Discussion & Comments
  - Ryan Witt, Managing Director, Healthcare Industry Practice - Proofpoint
  - Martin Littmann, Chief Technology Officer & CISO - Kelsey-Seybold Clinic
- Questions & Answers

Housekeeping Issues

- All participants are muted
  - To ask a question or make a comment, please submit via the Q&A feature and we will address as many as possible after the presentations.
- Technical difficulties:
  - Use the chat box and we will respond as soon as possible
- Today's slides will be available for download on eHI's Resource page **www.ehidc.org/resources**

Our Mission

eHealth Initiative's mission is to serve as the industry leader convening executives from multi-stakeholder groups to identify best practices to transform healthcare through use of technology and innovation. eHI conducts, research, education and advocacy activities to support the transformation of healthcare.

Multi-stakeholder Leaders in Every Sector of Healthcare

AMA
AMERICAN MEDICAL ASSOCIATION
American Cancer Society
Bristol-Myers Squibb
GE
imagination at work
salesforce
TELADOC
MAYO CLINIC
pwc
HL7 INTERNATIONAL
American Hospital Association
UnitedHealthcare
Cerner
Marshfield Clinic
HEALTH SYSTEM
Johnson & Johnson
aetna
surescripts

eHealth Resource Center Available With Best Practices & Findings

Best Practice Committees contribute to the eHealth Resource Center **www.ehidc.org/resources** which provides assistance, education and information to organizations transforming healthcare through the use of information, technology and innovation. The Resource Center is a compilation of reports, presentations, survey results, best practices and case studies from the last 16 years.

Save the Date: February 7 – 8, 2018
Top of the Hill, Washington, DC

eHealth Initiative Executive Summit

Convening Executives To Research & Identify Best Practices

Best Practice Committees Identify & Disseminate Success Stories

- VALUE & REIMBURSEMENT
- DATA ACCESS & PRIVACY
- WORKFLOW & PATIENT EXPERIENCE

proofpoint®

2018 GUIDE TO BUILDING YOUR SECURITY STRATEGY

Ryan Witt

Managing Director, Healthcare Industry Practice - Proofpoint

Martin Littmann

Chief Technology Officer & CISO - Kelsey-Seybold Clinic

Proofpoint at a Glance

LEADING CUSTOMERS

>50%
of the Fortune 100

5000+
enterprise customers

90%+
renewal rate

DEEP SECURITY DNA

100+
threat ops and research team

~20%
revenue invested in R&D

300K+
daily malware samples

UNIQUE VISIBILITY

1B+
messages processed daily

500B+
node threat graph

50M+
mobile apps scanned

ENTERPRISE CLASS

8
straight years of MQ leadership

paloalto NETWORKS

splunk>

CYBERARK

IMPERVA

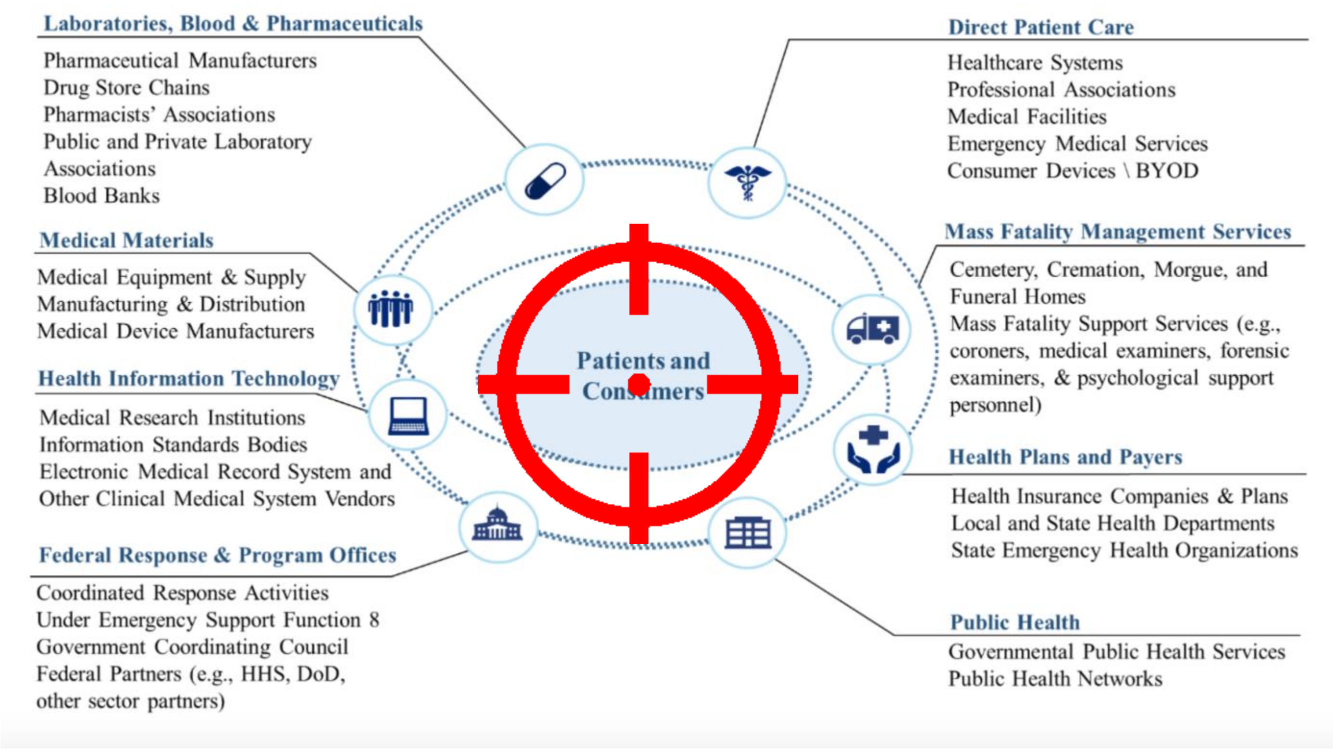
strategic ecosystem integrations

STATE OF THE UNION

HEALTHCARE CYBERSECURITY

Healthcare – Constant Attack State

Figure 2 Health Care Ecosystem



Laboratories, Blood & Pharmaceuticals

Pharmaceutical Manufacturers
Drug Store Chains
Pharmacists' Associations
Public and Private Laboratory Associations
Blood Banks

Medical Materials

Medical Equipment & Supply Manufacturing & Distribution
Medical Device Manufacturers

Health Information Technology

Medical Research Institutions
Information Standards Bodies
Electronic Medical Record System and Other Clinical Medical System Vendors

Federal Response & Program Offices

Coordinated Response Activities Under Emergency Support Function 8
Government Coordinating Council
Federal Partners (e.g., HHS, DoD, other sector partners)

Patients and Consumers

Direct Patient Care

Healthcare Systems
Professional Associations
Medical Facilities
Emergency Medical Services
Consumer Devices \ BYOD

Mass Fatality Management Services

Cemetery, Cremation, Morgue, and Funeral Homes
Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

Health Plans and Payers

Health Insurance Companies & Plans
Local and State Health Departments
State Emergency Health Organizations

Public Health

Governmental Public Health Services
Public Health Networks

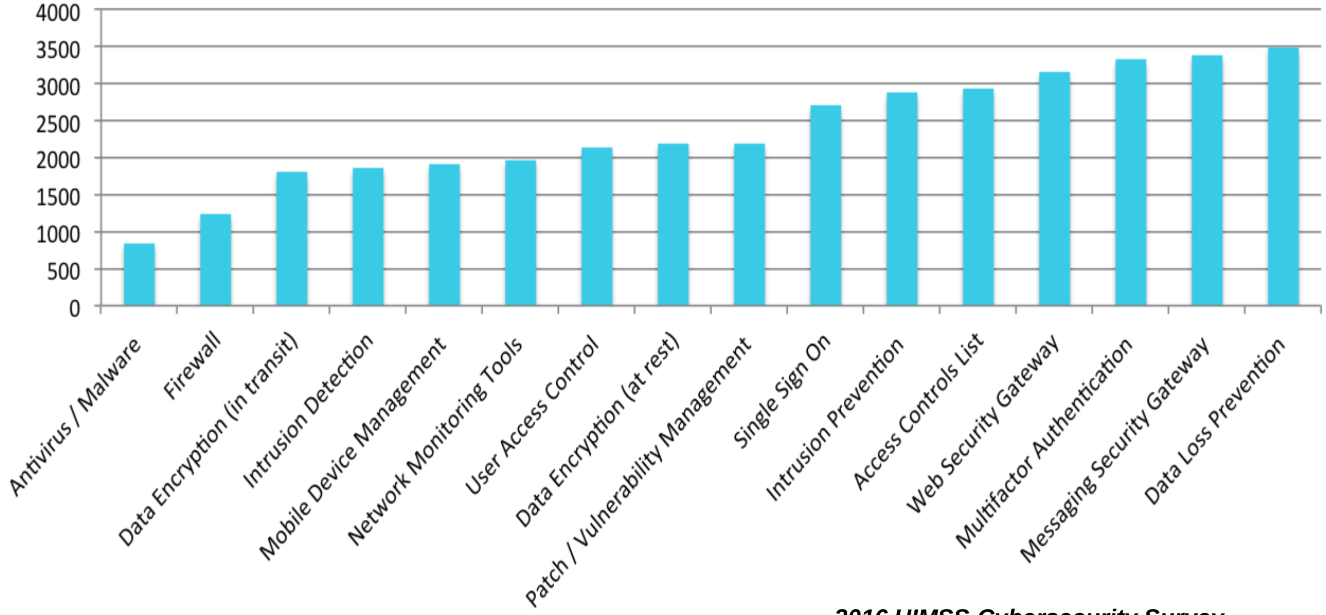
High Value of ePHI

Poor Security Posture

Healthcare Has Under Invested in InfoSec

54% of Healthcare believe that security technology is adequate

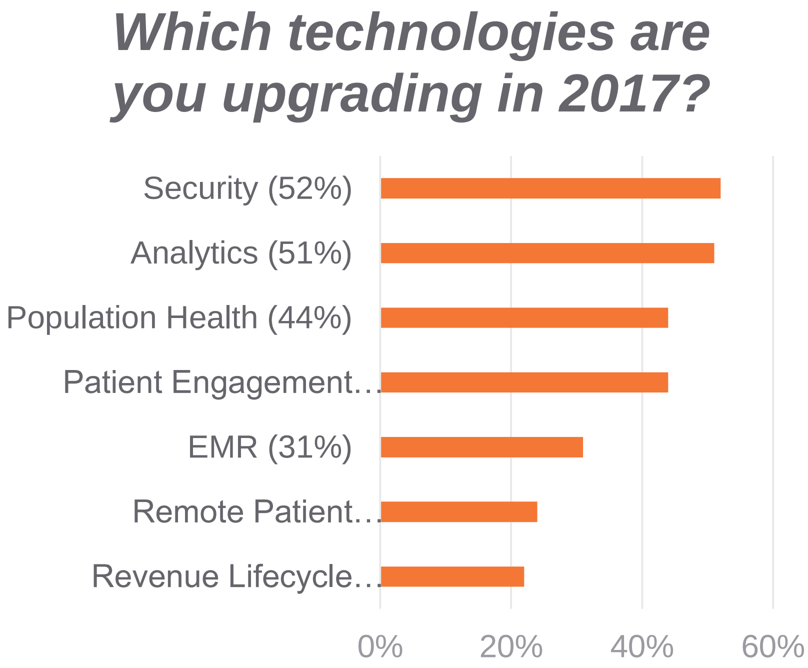
Number of US Acute Care Hospitals **Without** Deployed Security Technology

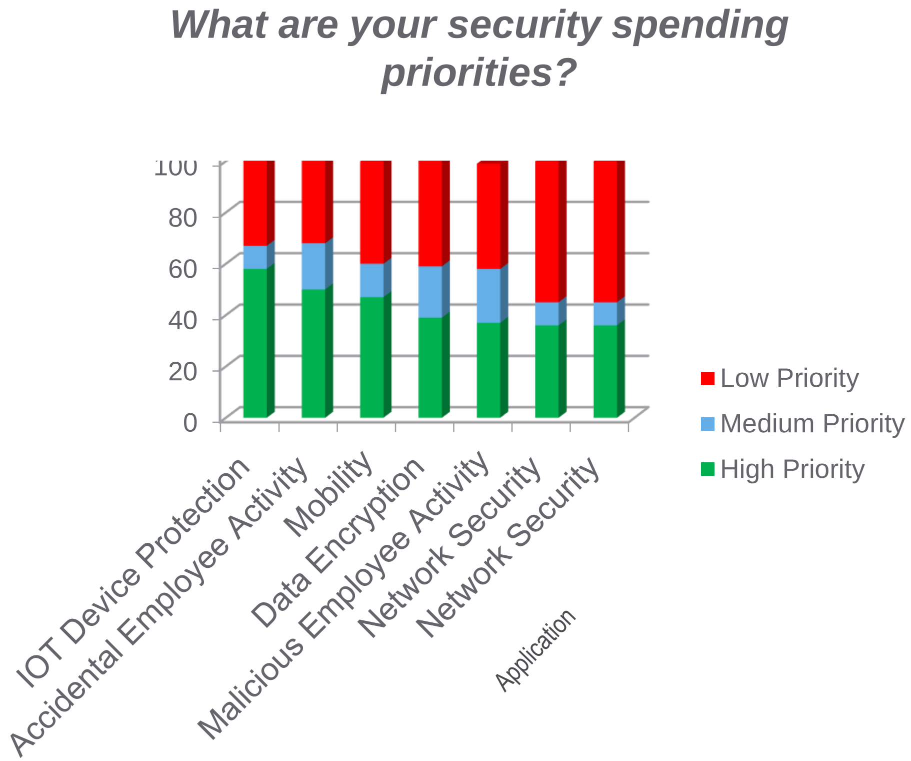


2016 HIMSS Cybersecurity Survey

2017 – “The Year Ahead in Health IT”

Healthcare IT News





Credential Phishing

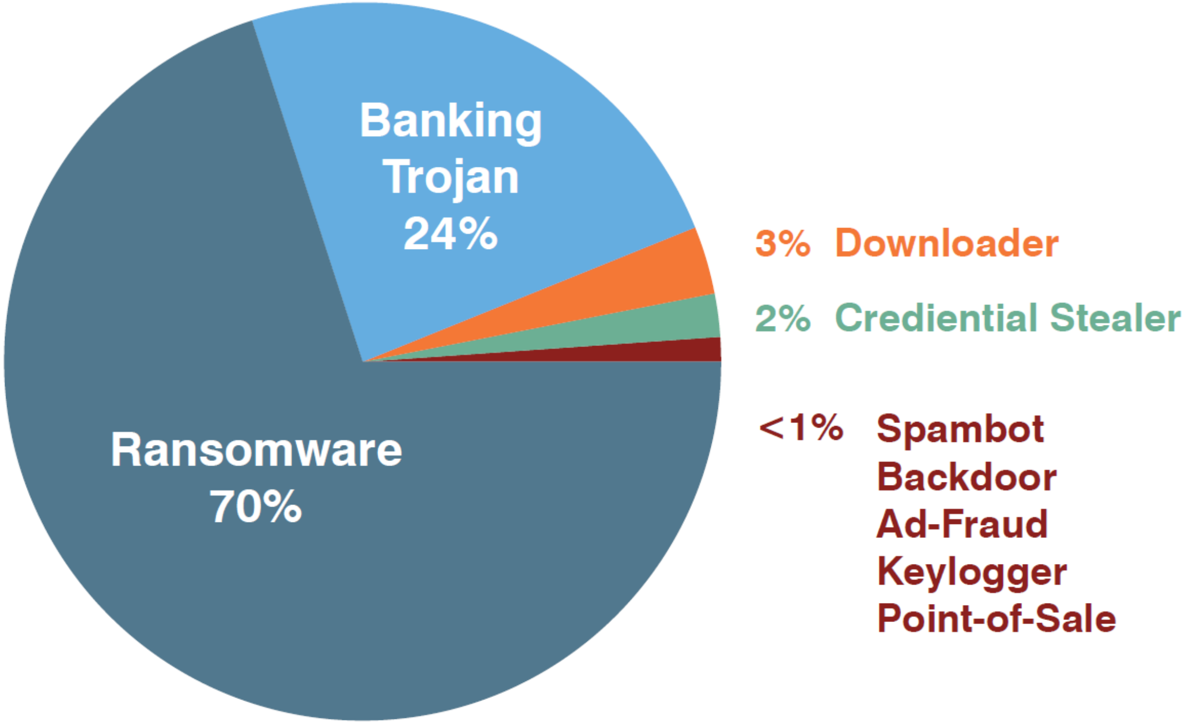
- Cyber criminals are carrying out **social engineering at scale**
- Highly personalized, targeted email campaigns have been focusing on **exploiting people**, and not just technology
- Credential phishing pages made up more than **90% of URL-based threats**
- Half of the clicks on malicious URLs occur outside enterprise desktop management

Business Email Compromise (BEC)

- BEC attacks catch up to banking Trojans
- Attackers use people, rather than binaries, to steal funds
- Attackers **mimic trusted brands** / use misleading domains

↑ 45% Quarter-over-quarter increase in BEC attacks in Q4

Ransomware the Dominant Email Payload of 2016



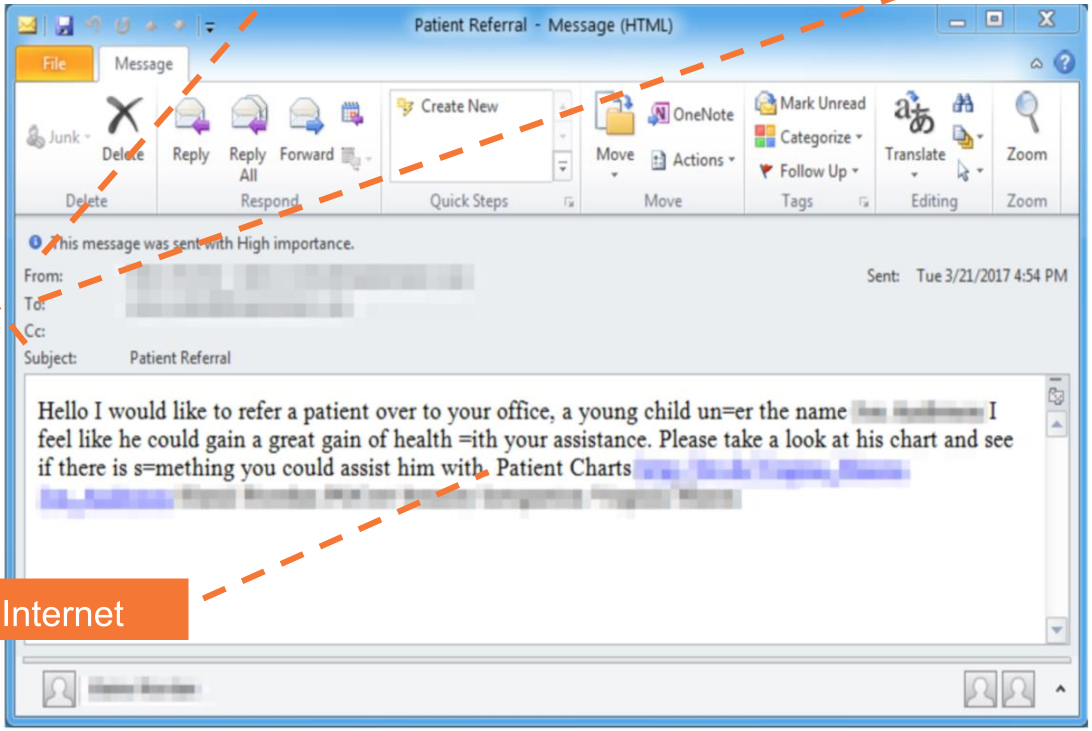
Proofpoint Human Factor Report, 2017

Healthcare Specific Ransomware

Patient Referral – Typical Use Case

Patient's Physician Listed

Specialist Practitioner Listed



This message was sent with High importance.

From: [redacted]

Sent: Tue 3/21/2017 4:54 PM

To: [redacted]

Cc:

Subject: Patient Referral

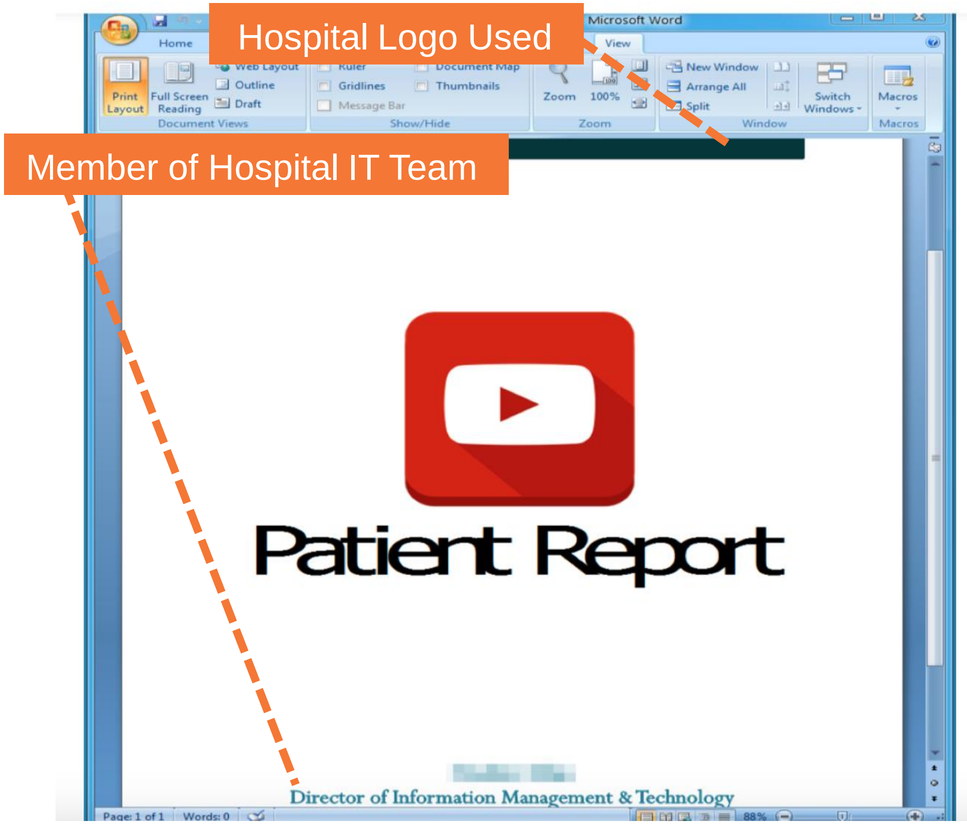
Hello I would like to refer a patient over to your office, a young child un=er the name [redacted] I feel like he could gain a great gain of health =ith your assistance. Please take a look at his chart and see if there is s=mething you could assist him with. Patient Charts [redacted]

[redacted]

"Patient Chart" from Internet

Proofpoint Human Factor Report, 2017

Defray – New Ransomware Targeting Healthcare



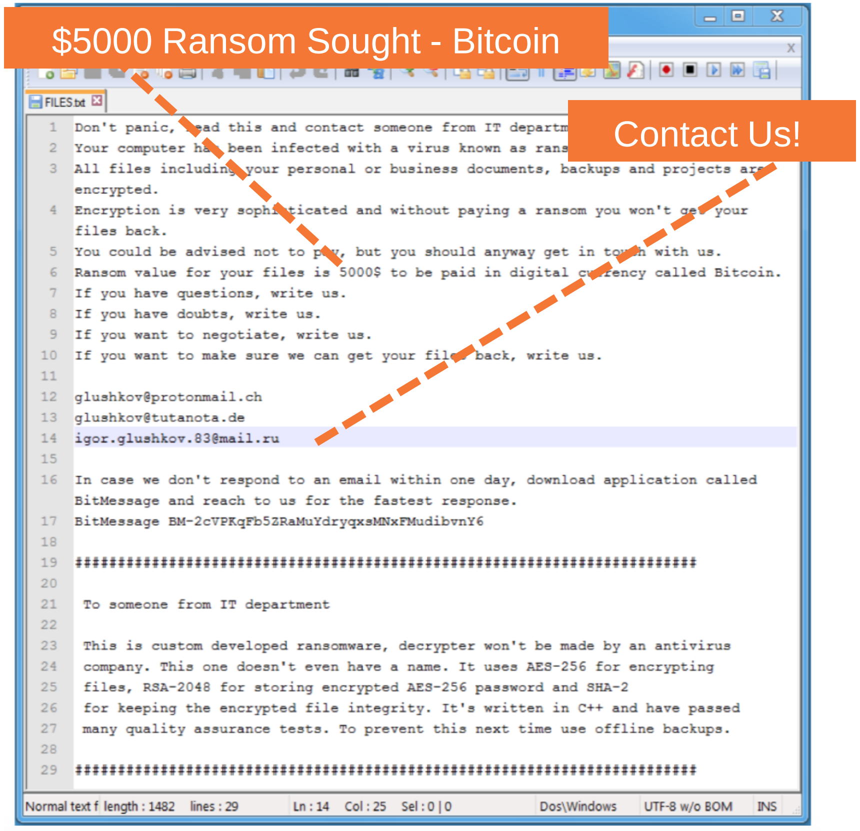
Patient Report

[redacted]

Director of Information Management & Technology

Hospital Logo Used

Member of Hospital IT Team



```
Don't panic, read this and contact someone from IT departm
Your computer has been infected with a virus known as rans
All files including your personal or business documents, backups and projects are
encrypted.
Encryption is very sophisticated and without paying a ransom you won't get your
files back.
You could be advised not to pay, but you should anyway get in touch with us.
Ransom value for your files is 5000$ to be paid in digital currency called Bitcoin.
If you have questions, write us.
If you have doubts, write us.
If you want to negotiate, write us.
If you want to make sure we can get your files back, write us.

glushkov@protonmail.ch
glushkov@tutanota.de
igor.glushkov.83@mail.ru

In case we don't respond to an email within one day, download application called
BitMessage and reach to us for the fastest response.
BitMessage BM-2cVPKqFb5ZRaMuYdryqxsMNxFMudibvnY6

#######################################################################

 To someone from IT department

 This is custom developed ransomware, decrypter won't be made by an antivirus
 company. This one doesn't even have a name. It uses AES-256 for encrypting
 files, RSA-2048 for storing encrypted AES-256 password and SHA-2
 for keeping the encrypted file integrity. It's written in C++ and have passed
 many quality assurance tests. To prevent this next time use offline backups.

#######################################################################
```

```
Normal text f  length : 1482   lines : 29   Ln : 14   Col : 25   Sel : 0 | 0   Dos\Windows   UTF-8 w/o BOM   INS
```

$5000 Ransom Sought - Bitcoin

Contact Us!

Protenus Breach Monitor (Healthcare) - 2017

180 Days / 180 Breaches	% of Breaches from Hacking	# Days Before Reporting Breach to HHS	# Days Before Breach Discovered
1.000	53	54	326

2017 Cost of Data Breach Study – Highlights

Figure 4. Per capita cost by industry

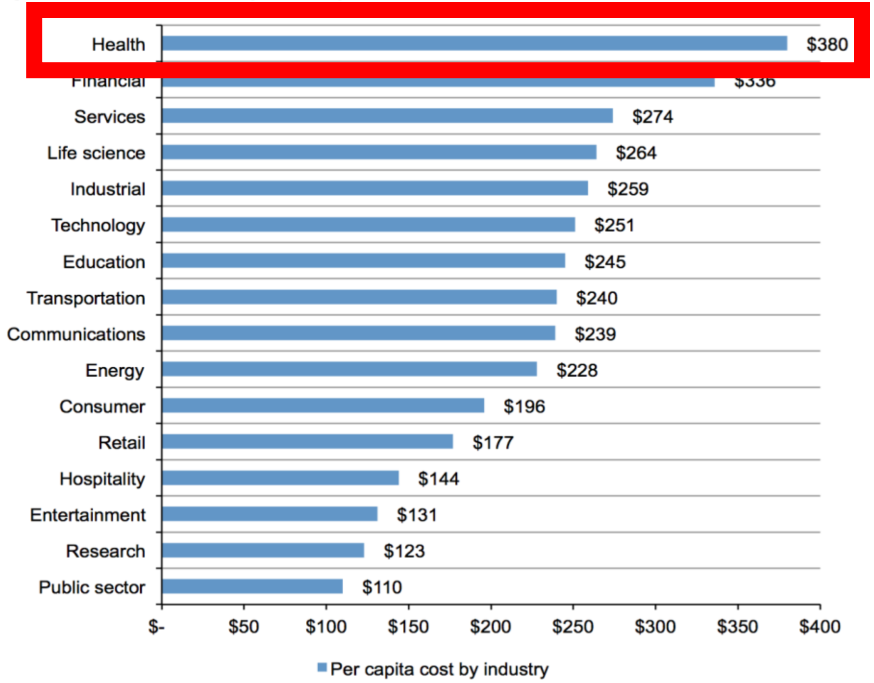
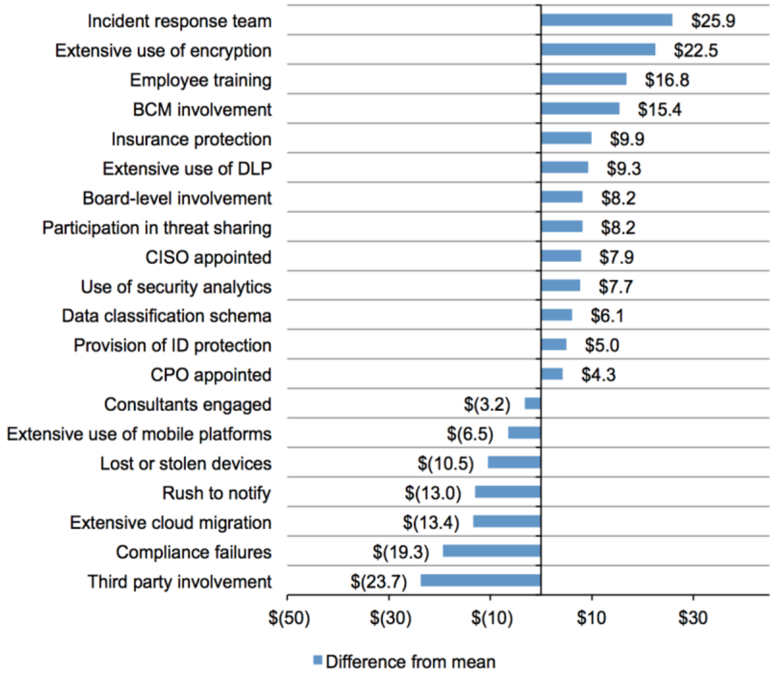


Figure 7. Impact of 20 factors on the per capita cost of data breach



Ponemon Highlights – Part 2

Technology Investments POST Breach

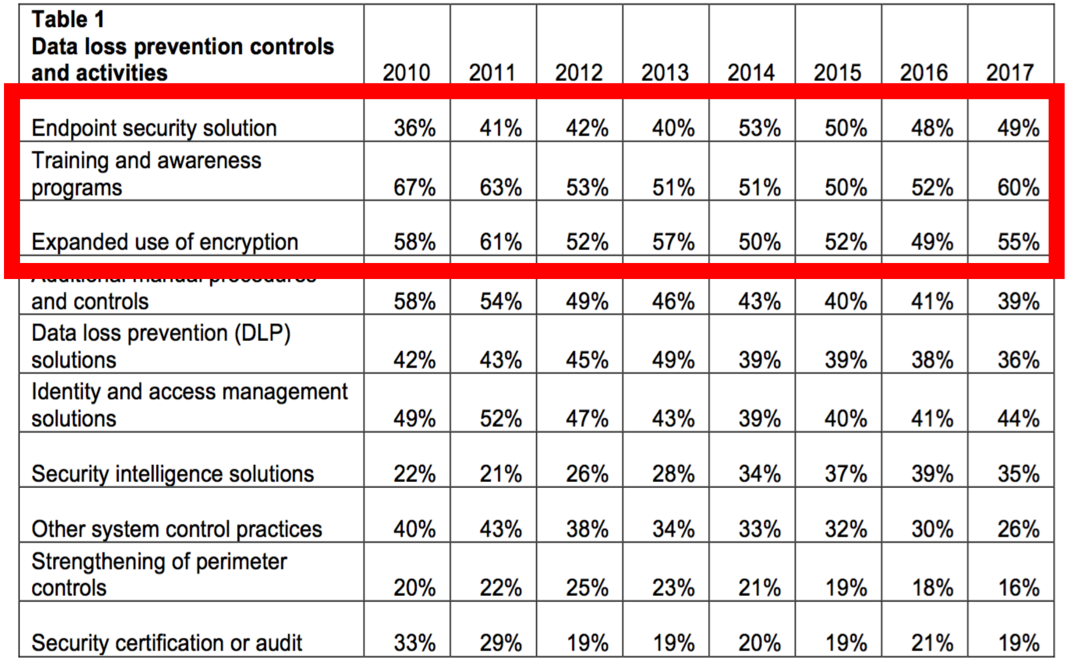


Table 1 Data loss prevention controls and activities	2010	2011	2012	2013	2014	2015	2016	2017
Endpoint security solution	36%	41%	42%	40%	53%	50%	48%	49%
Training and awareness programs	67%	63%	53%	51%	51%	50%	52%	60%
Expanded use of encryption	58%	61%	52%	57%	50%	52%	49%	55%
Additional manual procedures and controls	58%	54%	49%	46%	43%	40%	41%	39%
Data loss prevention (DLP) solutions	42%	43%	45%	49%	39%	39%	38%	36%
Identity and access management solutions	49%	52%	47%	43%	39%	40%	41%	44%
Security intelligence solutions	22%	21%	26%	28%	34%	37%	39%	35%
Other system control practices	40%	43%	38%	34%	33%	32%	30%	26%
Strengthening of perimeter controls	20%	22%	25%	23%	21%	19%	18%	16%
Security certification or audit	33%	29%	19%	19%	20%	19%	21%	19%

*Please note that a company may be implementing more than one preventive measure.

Figure 19. Days to identify and contain the data breach by root cause

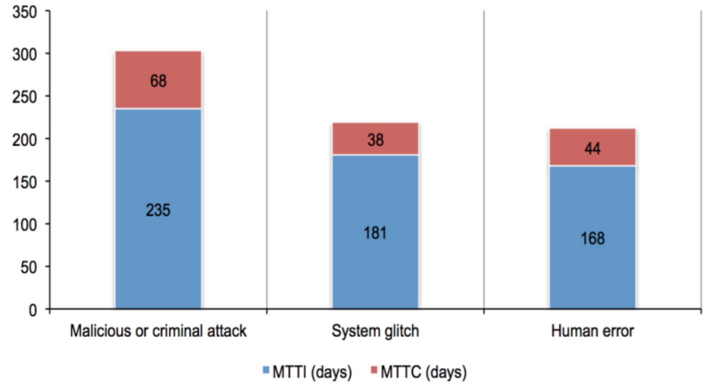
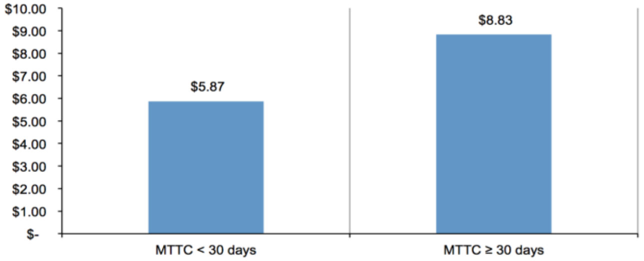


Figure 18. Mean time to contain and average total cost
Measured in US$ (millions)



Experian Report

2017 DATA BREACH INDUSTRY FORECAST

1. "Aftershock" password breaches will expedite the "death of the password"
2. Nation-State Cyber-Attacks will move from espionage to war
3. Healthcare organizations will be the most targeted sector with new, sophisticated attacks emerging
4. Criminals will continue to focus on payment based attacks despite the shift in EMV occurring
5. International data breaches will cause big headaches for multinationals

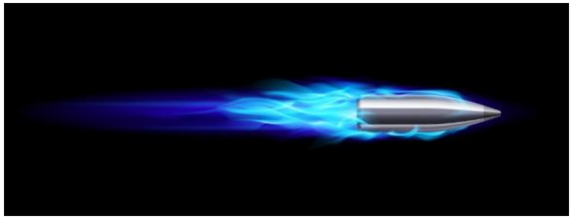
2018 Guide to Your Security Strategy

Guiding Principles

- IT Security is here to protect the Business and enable stable Operations
- Delicate and Artful Balance when Business Needs and Security needs conflict
- IT Security is Everybody’s Responsibility
- We will invest in Security Resources and Achieve results consistent with Healthcare Industry Benchmarks

There are no Silver Bullets

- Security is a process and not an achievement
- Success is a combination of people, process, and technology
- Avoid ROI Thinking
- Insurance Mentality
- Demonstrable Results should be expected
- Prioritize investments

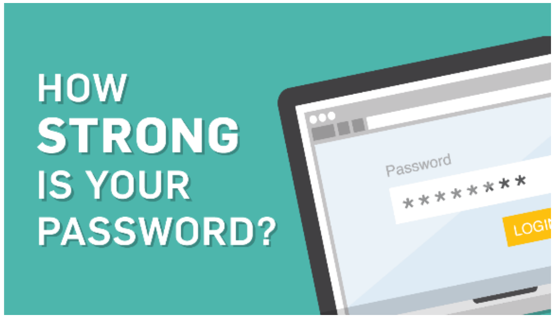


Processes

- USB Management
  - Encryption
  - MTP/PTP protocols
  - Read-only policies
- Geo blocking
- Data loss protection
  - Block personal mail or block attachments
  - Block peer to peer file sharing
- Automation of reboots or lockdown upon infection
- Password Policy

Password Policy – NIST Guidance

- 12/14 character minimum
- No “complexity” required
- Long life (1 year)
- Dictionary for un-allowed passwords, patterns
- Forced reset on compromise
  - Phishing – test or real
  - Lost/stolen device
  - Sharing
- Guidance not to re-use for any personal accounts



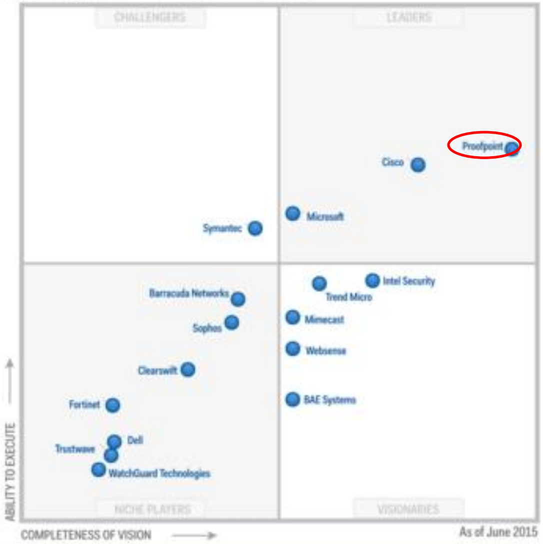
Security Program Components

- Staffing & Executive Sponsorship
- Layered Defense and Resiliency Strategy
- Security Tools, Technologies, Services
  - Firewall
  - DNS Protection
  - Email Security
  - Malware Detection & Prevention
  - Two Factor Authentication
  - PHI Monitoring
  - Incident Response
  - Education & Testing

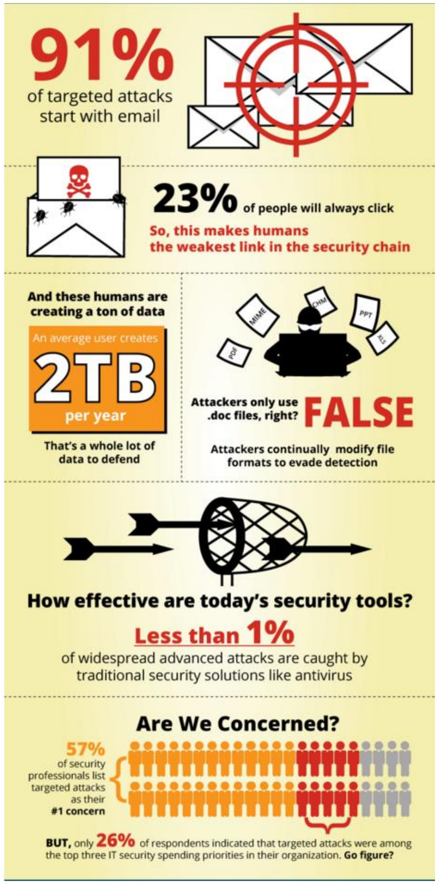
ProofPoint – Email Security

- Spam & Malware protection
- Email Classification & Tagging
- Attachment Defense
- URL Re-writes
- Sandboxing
- Encryption
- Secure File Sharing
- Fraud protection
- (and Threat Response!)

Figure 1. Magic Quadrant for Secure Email Gateways



Source: Gartner (June 2015)



91% of targeted attacks start with email

23% of people will always click

So, this makes humans the weakest link in the security chain

And these humans are creating a ton of data

An average user creates 2TB per year

That's a whole lot of data to defend

Attackers only use .doc files, right? FALSE

Attackers continually modify file formats to evade detection

How effective are today's security tools?

Less than 1% of widespread advanced attacks are caught by traditional security solutions like antivirus

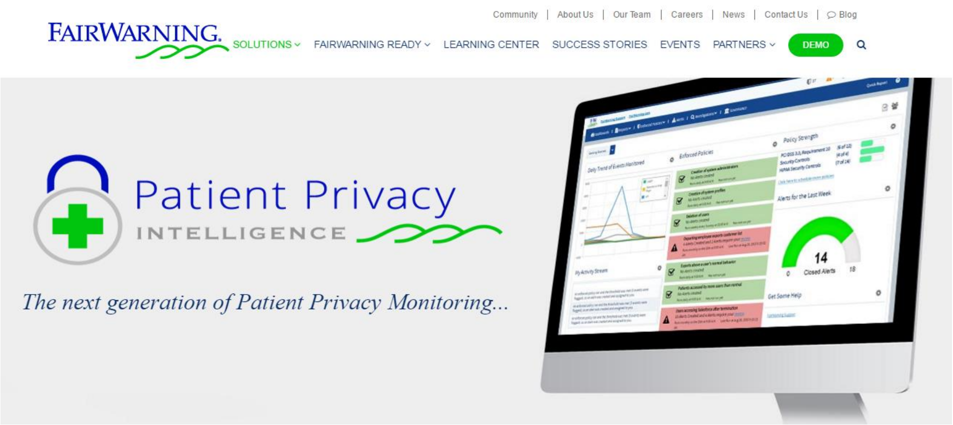
Are We Concerned?

57% of security professionals list targeted attacks as their #1 concern

BUT, only 26% of respondents indicated that targeted attacks were among the top three IT security spending priorities in their organization. Go figure?

FairWarning

- Provides monitoring the progress of investigations/incidents and reporting on resolution activities.
- Detection & alerting of inappropriate PHI access
- Consolidate view of PHI access
- Provides PHI access investigation tool
- Current Alerts
  - ✓ Deceased Patient Record Access
  - ✓ EPIC Restricted Patient Access
  - ✓ Family Member Snooping
  - ✓ Supervisor Snooping
  - ✓ Meds Order Alerts
  - ✓ Self Modification



Patient Privacy INTELLIGENCE

The next generation of Patient Privacy Monitoring...

Identity Management

- Privileged Account Management
- Active Directory tools
- Two Factor Authentication
- Single Sign On
- EPCS

Risk & Penetration Assessments

- 3rd Party HIPAA audit
- Based on NIST SP 800-115 and HITRUST CSF
- Identifies gaps and areas for improvement
- Penetration Test
  - identify exploitable security vulnerabilities and insufficiently configured security controls to determine the likelihood that an individual with little or no prior knowledge of the environment (e.g., an uninformed outsider or an insider) could obtain unauthorized access to an entity’s Internet-facing and internal resources

Phishing Program

- Regularly test/train users
- Craft test to match current actual threats
- Run same test multiple times
- Educate AND “penalize” offenders
- Support program with awareness education
  - Intranet postings
  - Signage
  - All-User emails (leverage current incidents)

Questions?

proofpoint®

Questions and Answers

Ryan Witt
Managing Director, Healthcare Industry Practice - Proofpoint

Martin Littmann
Chief Technology Officer & CISO - Kelsey-Seybold Clinic