Ransomware attacks and protecting patient data: What can we learn from WannaCry?
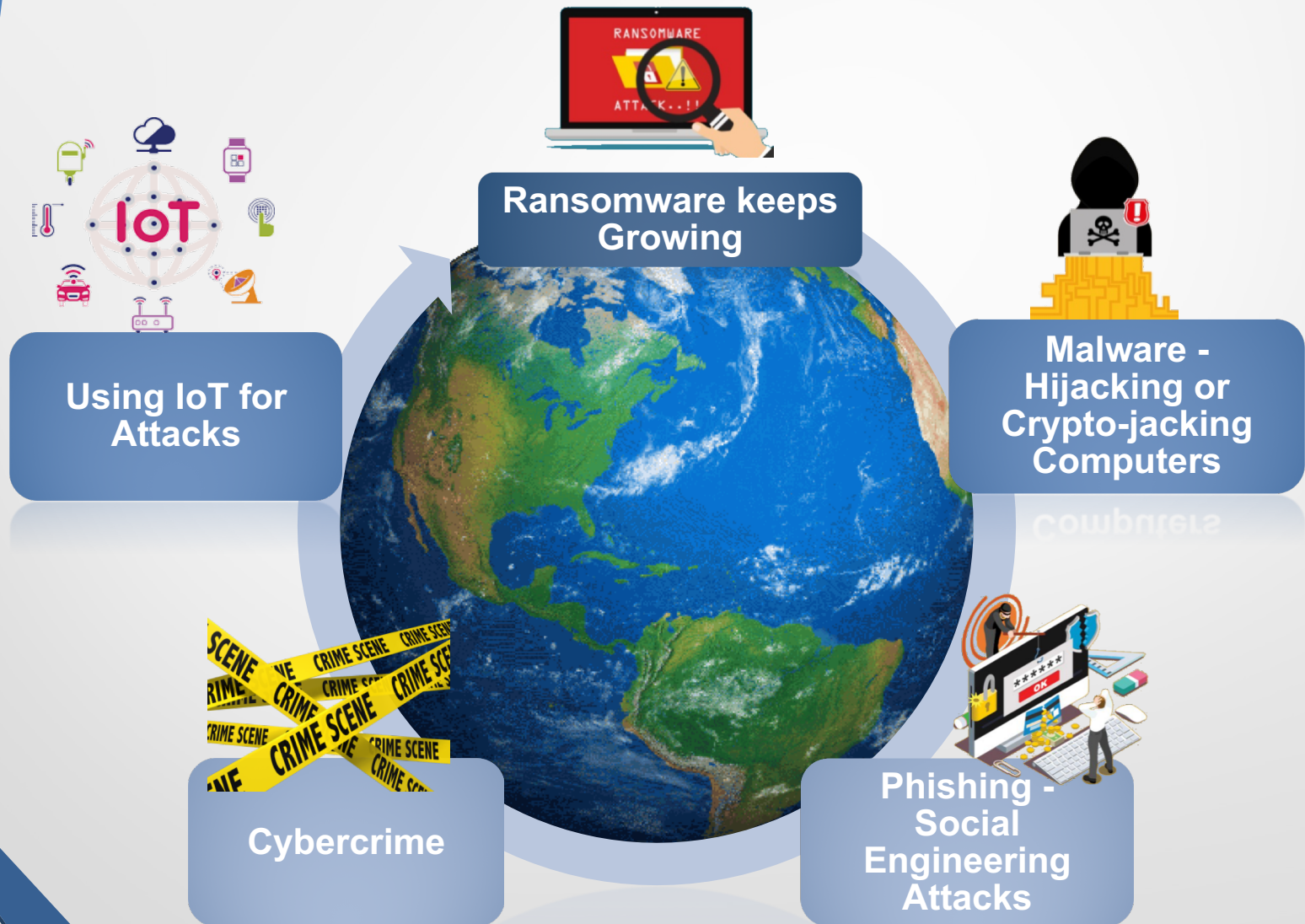
7/17/2018

Sanjay Deo, CISSP, HCISPP

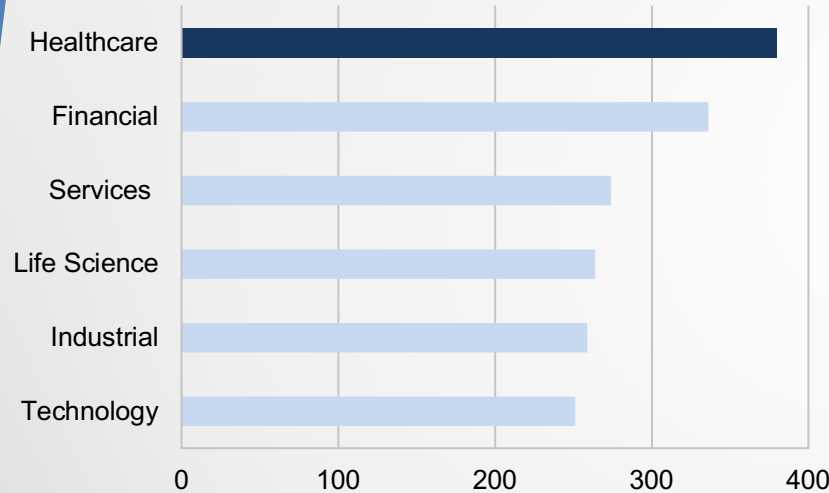Founder and President

CYBER RISK TRENDS IN THE WORLD

Ransomware keeps Growing

Malware - Hijacking or Crypto-jacking Computers

Using IoT for Attacks

Phishing - Social Engineering Attacks

Cybercrime

IoT – Internet of Things

CYBER RISKS TRENDS

Data breach cost per capita

By industry classification, 2017 ($)

Industry	Cost
Healthcare	~380
Financial	~335
Services	~275
Life Science	~265
Industrial	~260
Technology	~255

(chart x-axis: 0, 100, 200, 300, 400)

Total Internet Devices — **20** Billion

IoT Devices — **8.4** Billion

Global Population — **7.6** Billion

The World Economic Forum Organization has reported more IoT devices than Global Population

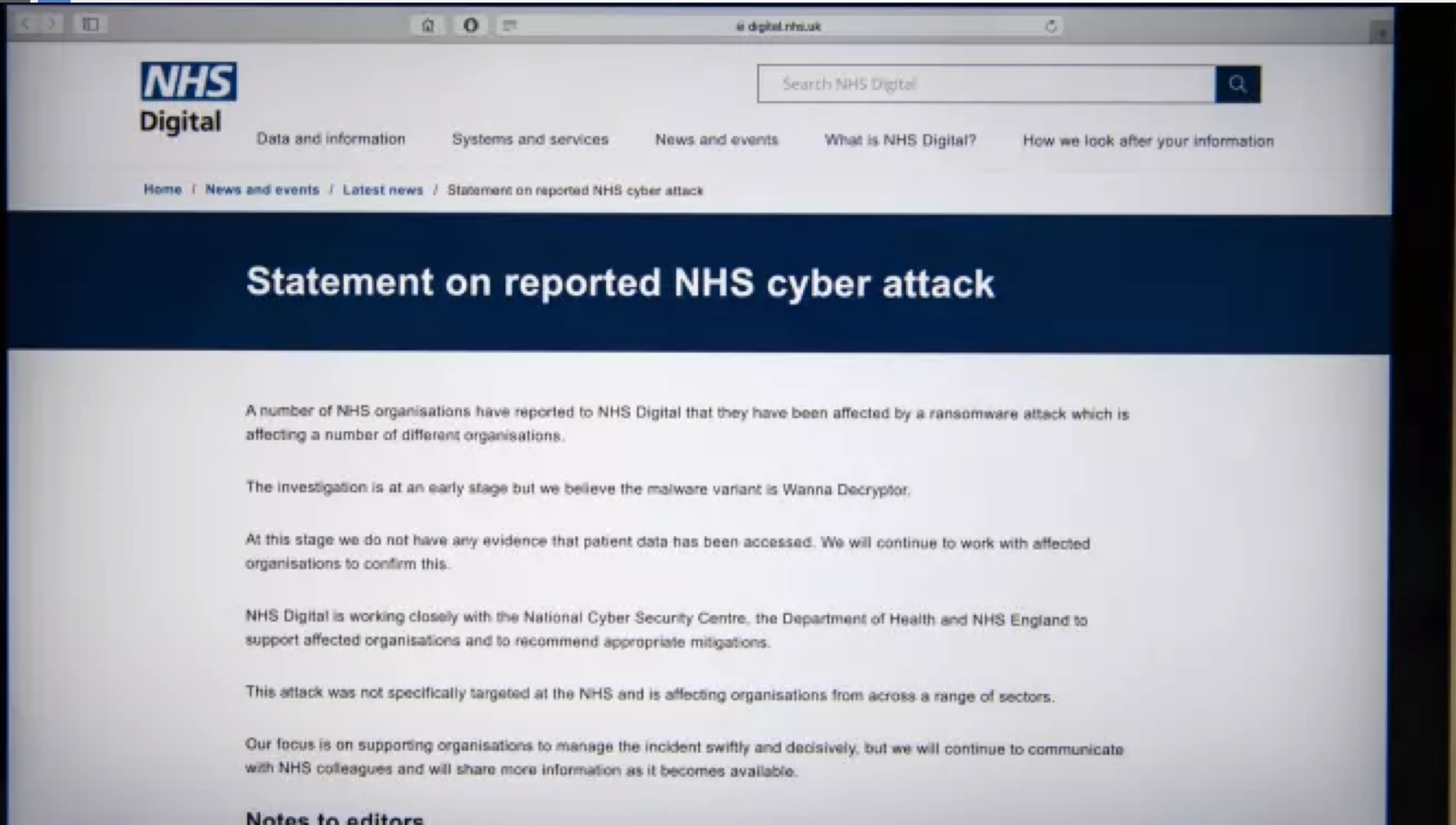**Global cyber-attacks in 2017, including WannaCry and Petya**

Wanna Cry

Petya

CYBER RISK IN HEALTHCARE

Lack of Knowledge of Cyber Security

High Demand of Medical Records in the Black Market

Healthcare Employee Negligence

HEALTHCARE

Medical staff usage of BYOD

Increase in Ransomware Attacks

WannaCry
May 12, 2017

WannaCry

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/15/2017 10:12:10

Time Left

02:23:55:10

Your files will be lost on

5/19/2017 10:12:10

Time Left

06:23:55:10

About bitcoin

How to buy bitcoins?
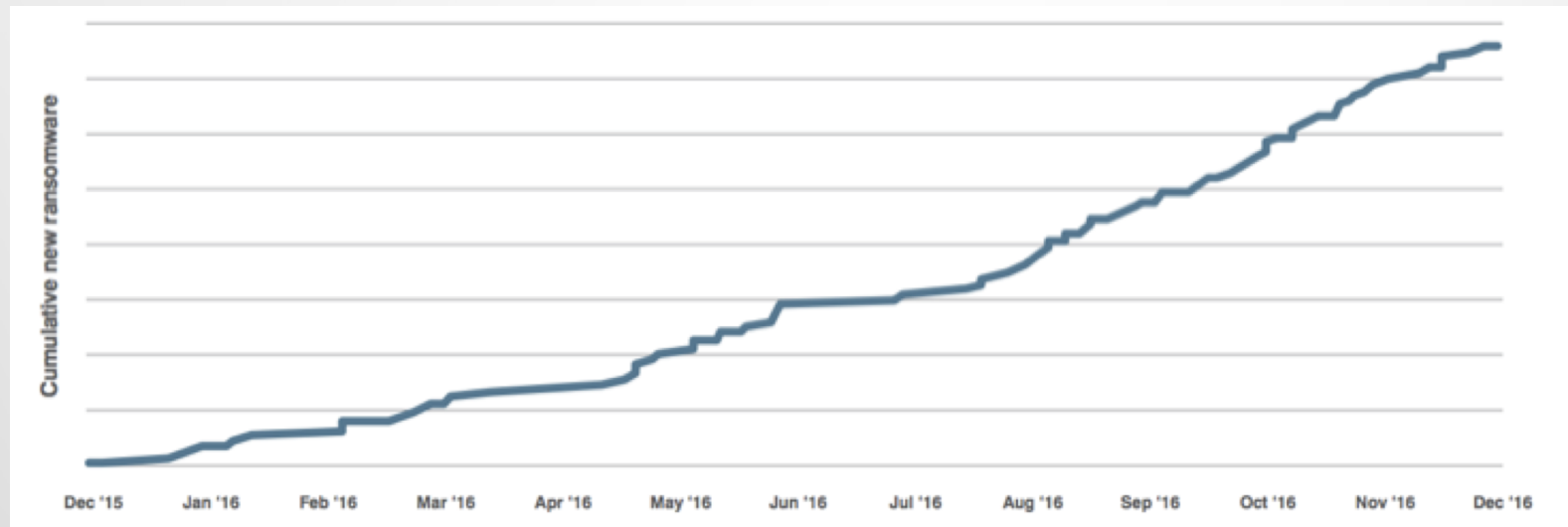
bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

Ransomware Attacks are Pervasive

Ransomware Variants Grew by **30x** in 2016

- A company gets hit every 40 seconds
- 50% of organizations attacked by ransomware are hit more than once
- Phishing email attachments are the #1 delivery vehicle

Ransomware Vectors

Impacted Data Source

Ransomware Vectors bar chart:
- Email Link — 31%
- Email Attachment — 28%
- A Web site or Web application other than email or social media — 24%
- Social Media — 4%
- USB Stick — 3%
- Business Application — 1%
- We Don't Know — 9%

Impacted Data Source pie chart:
- Endpoints — 60%
- Servers — 33%
- Cloud applications (e.g., Office 365 or Box) — 7%
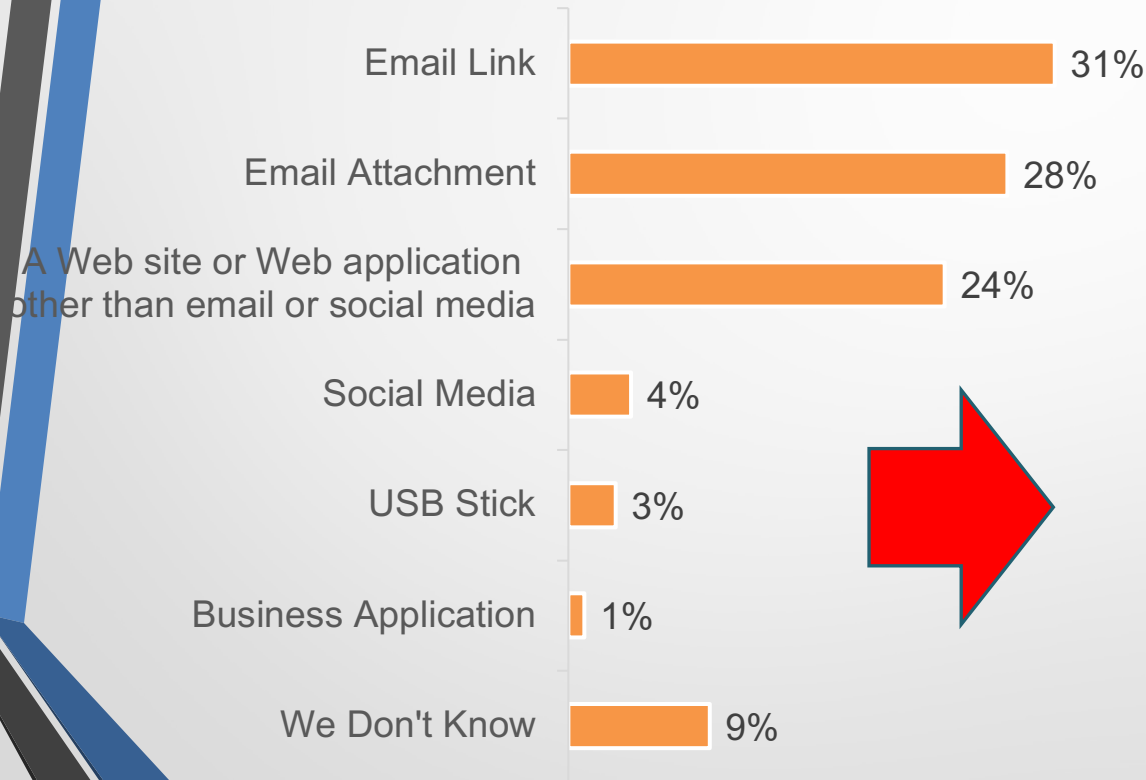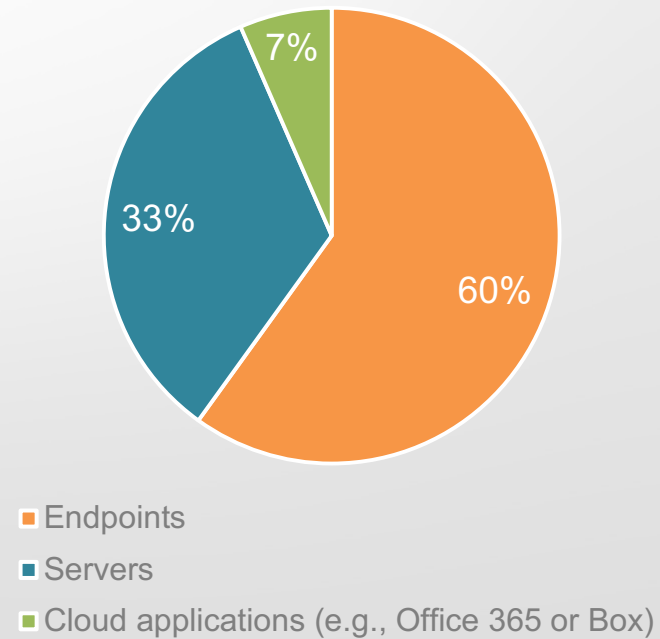
What is Ransomware & Stats?

- a type of malicious software designed to block access to a computer system until a sum of money is paid.

45%
of Ransomware attacks in 2017 targeted healthcare organizations

5 million
The cost of an average cyber attack now exceeds $5 million

7 out of 10
organizations don't believe their antivirus can stop the threats
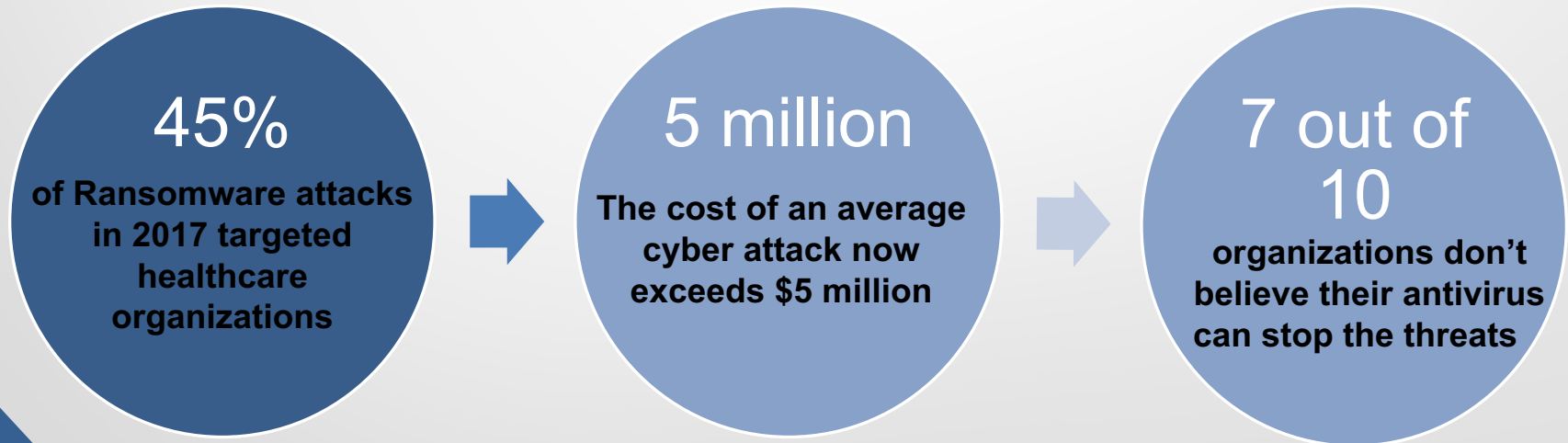
5 Common types of Ransomware?

Cerber
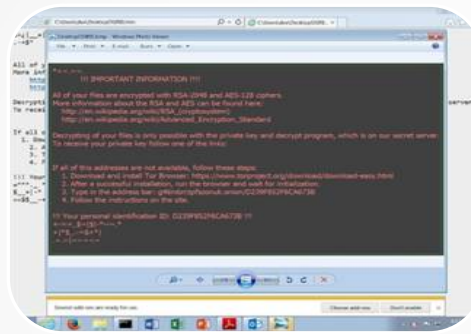
Locky

Samsam

Cryptowall

Crysis

Ransomware – Hollywood Presbyterian

"The reports of the hospital paying 9000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this." - Allen Stefanek, President and CEO, Hollywood Presbyterian Medical Center
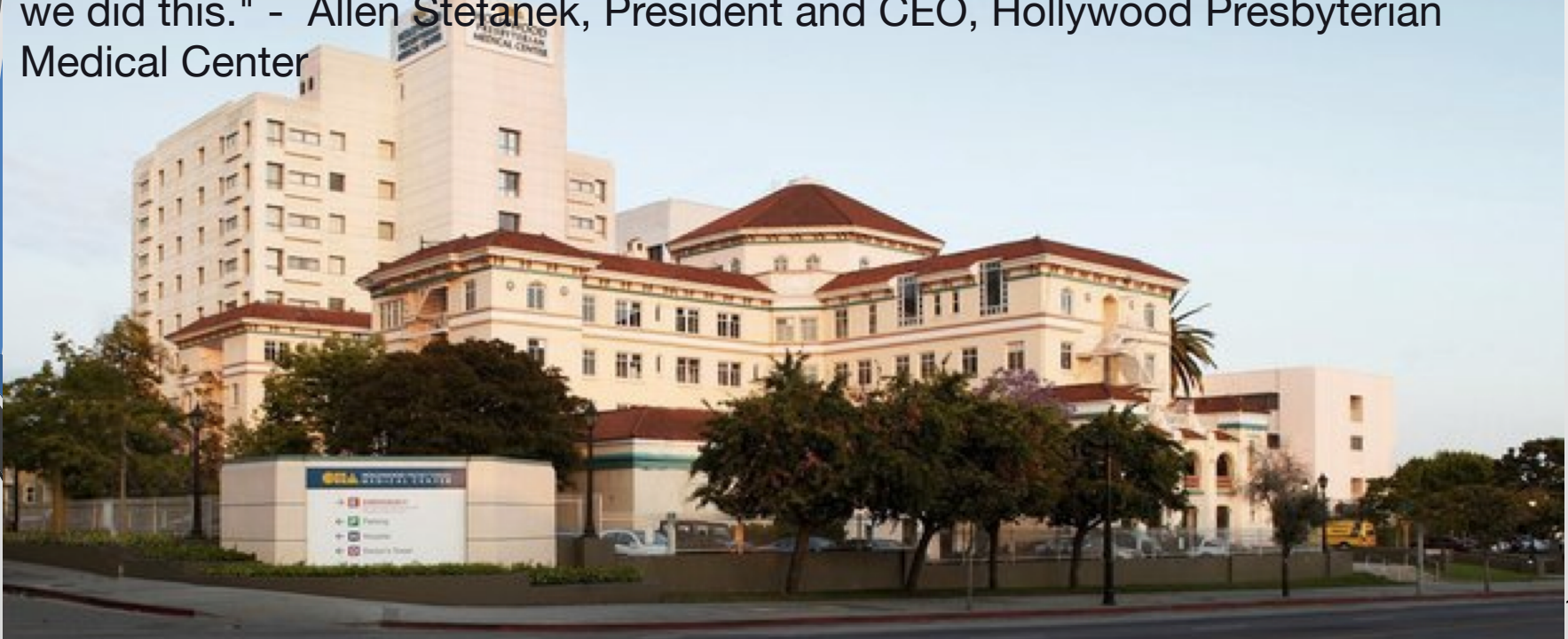
Ransomware Myth
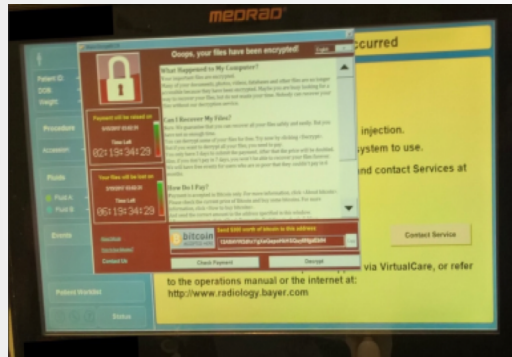
Only 42%
of companies report being able to fully recover data after an attack

Kansas Heart Hospital was hit with a ransomware attack on 18th of May 2016

"It paid the ransom, but then attackers tried to extort a second payment."

Ransomware Attacks

Bayer MedRad device was the first medical device infected in the United States with Ransomware

June 2017, a group of Hackers in Ukraine launched the "Petya" Ransomware attack against multiple international companies.

Ransomware 2018

July

- Cass Regional Medical Center recovering from a ransomware attack Monday, July 9th 2018 at 10 am and struck its communication system

February

- The California-based Center for Orthopedic Specialists (COS) is notifying 85,000 of its current and former patients that a ransomware attack on its IT vendor may have breached their data.
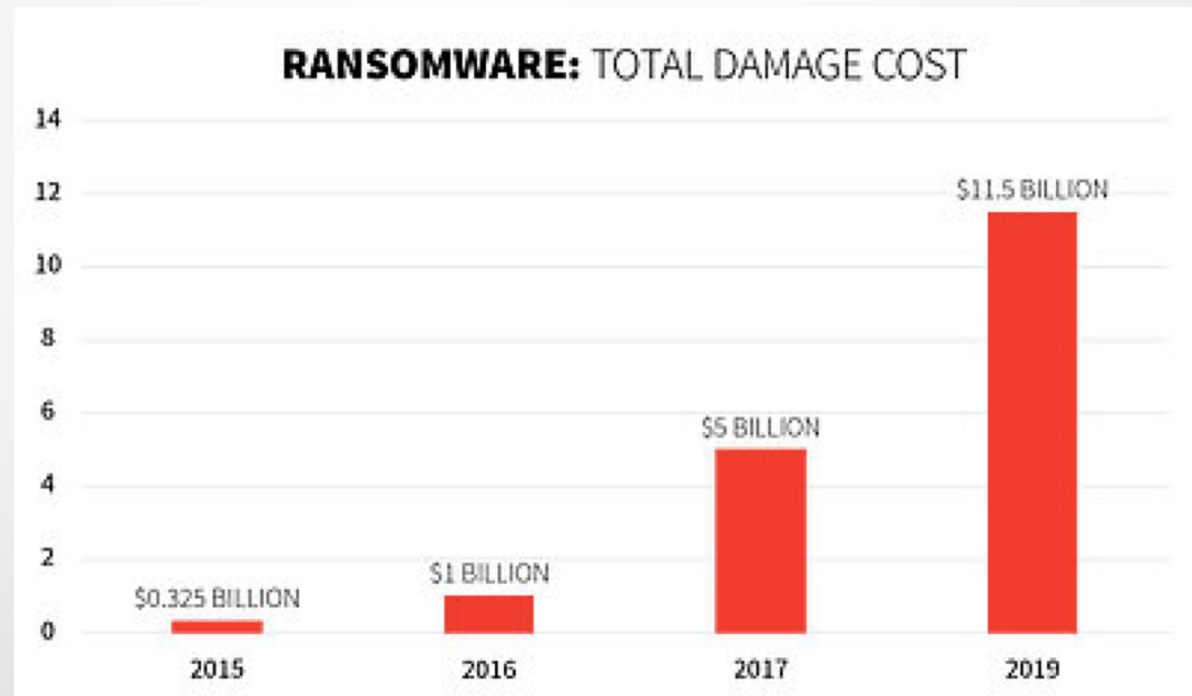
January

- A limited number of Allscripts services went down January 2018 after a ransomware incident

Ransomware Impact

- Data loss
- Operation Downtime
- Resetting and replacing infrastructure
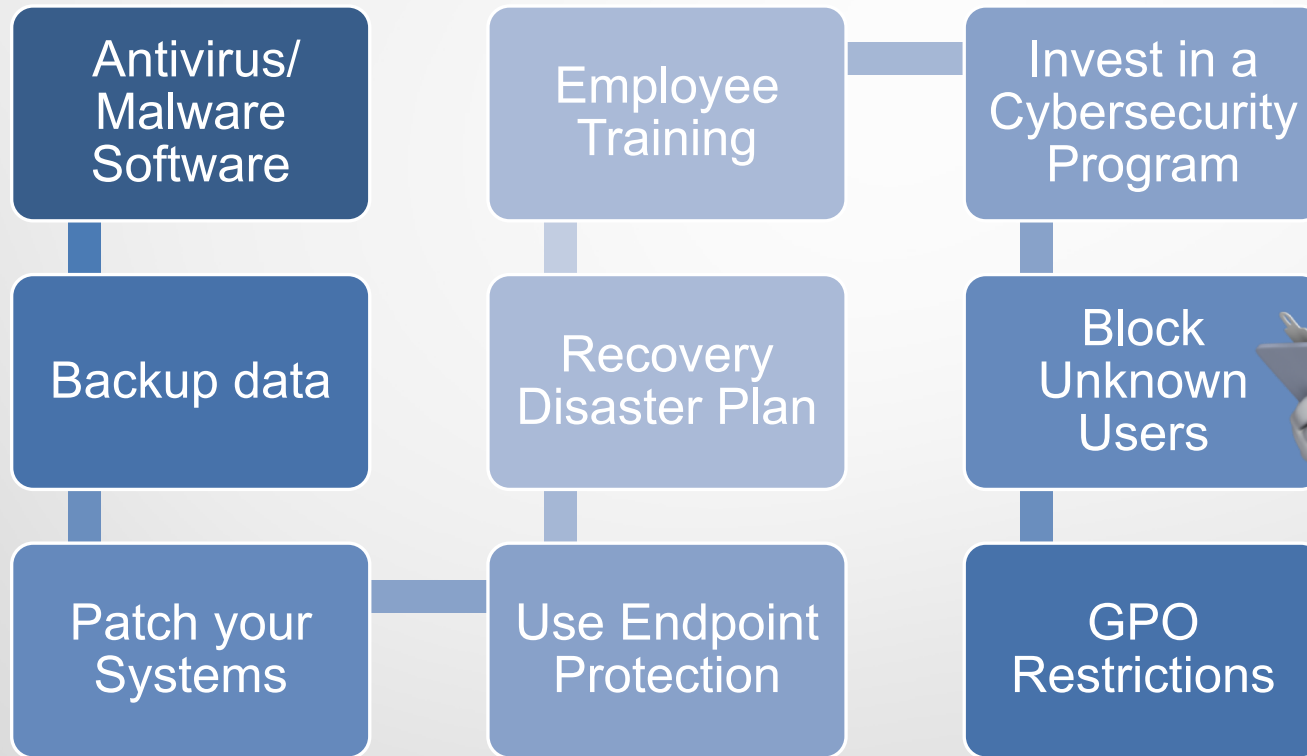- Productivity
- Forensics
- Reputation
- Life

RANSOMWARE: TOTAL DAMAGE COST

$0.325 BILLION (2015)
$1 BILLION (2016)
$5 BILLION (2017)
$11.5 BILLION (2019)

Estimated costs in damages from ransomware (Source: CyberSecurity Ventures)

Ransomware Mitigation

- Always back-up important files. It is recommended to save it in another device like external storage away from your local network. Another option for backing up your files is through the in-the-cloud system
- Keep your backups <u>disconnected</u> (unless you run the backup).
- Keep operating systems and software up-to-date, including security updates
- Implement end-user and network policy to mitigate risk of being attacked from external and internal sources
- Don't click the links and download file attachments from malicious website and suspicious e-mails respectively
- Disable auto-execution of scripts such as macros, javascript

How to protect patient data

Antivirus/ Malware Software

Backup data

Patch your Systems

Employee Training

Recovery Disaster Plan

Use Endpoint Protection

Invest in a Cybersecurity Program

Block Unknown Users

GPO Restrictions

CONTACT INFORMATION

(844) 55-CYBER (29237)

Sanjay.Deo@24by7security.com

Contact@24by7security.com

www.24By7Security.com

@24By7Security