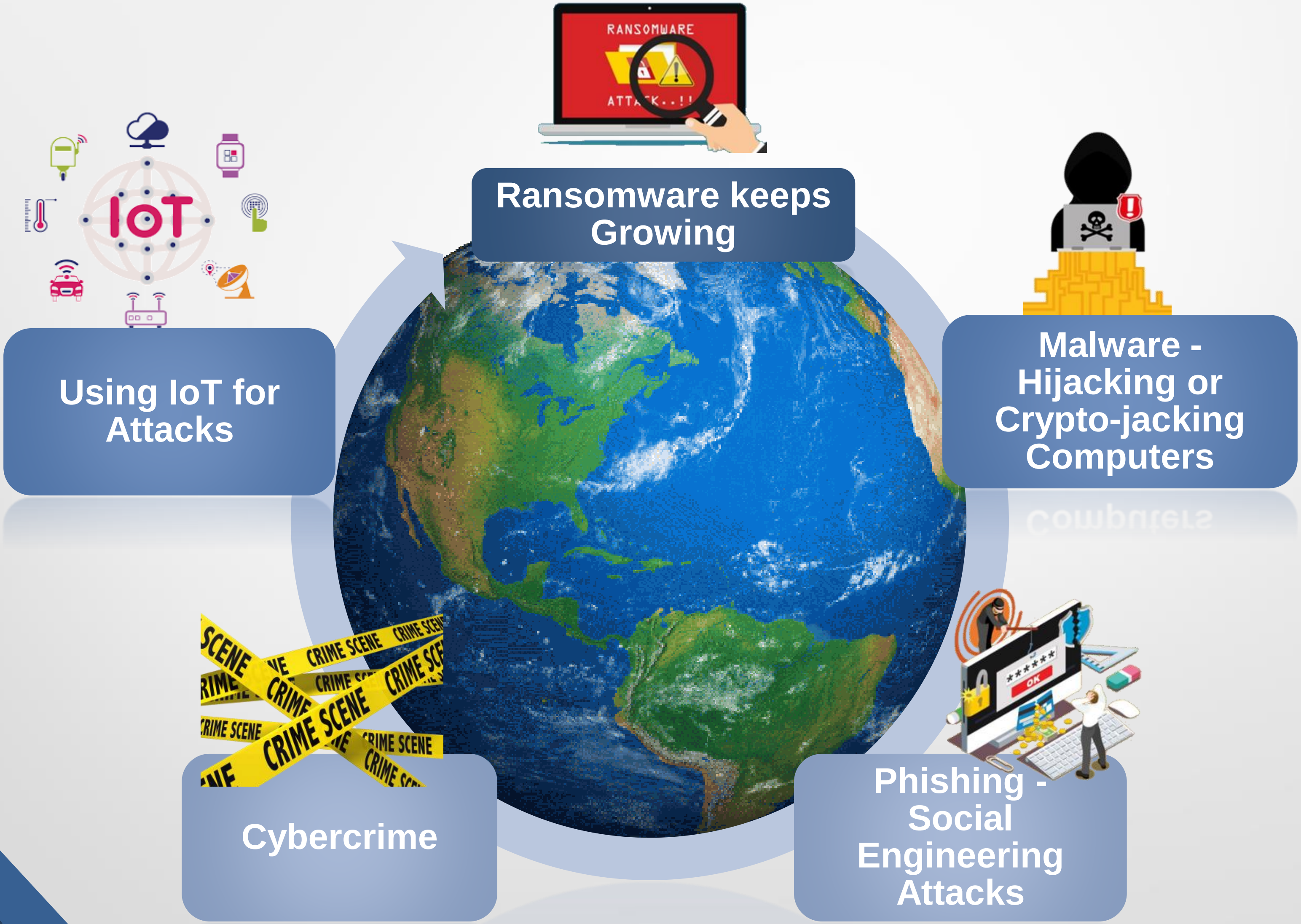
Ransomware attacks and protecting patient data: What can we learn from WannaCry?

Time Session: 4:30 pm
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

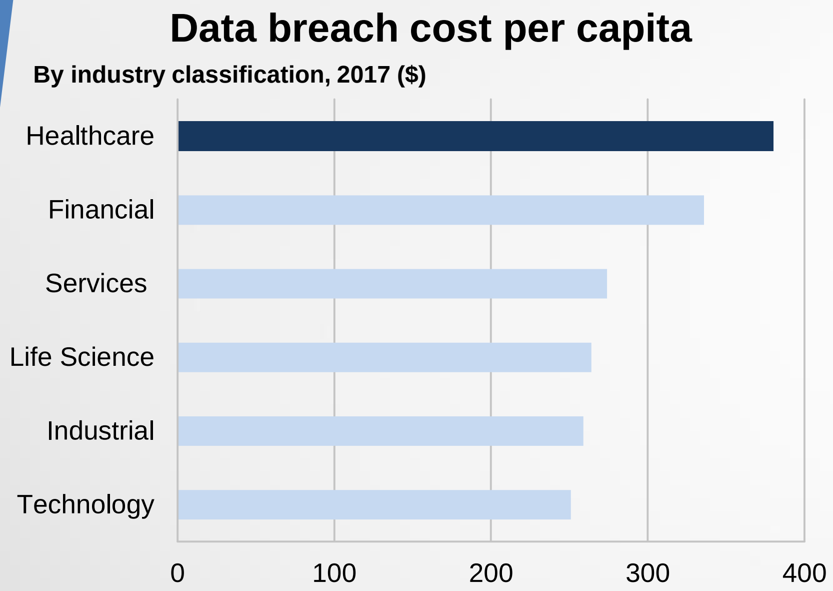
Phishing - Social Engineering Attacks

Cybercrime

Using IoT for Attacks

IoT – Internet of Things

CYBER RISKS TRENDS


Data breach cost per capita

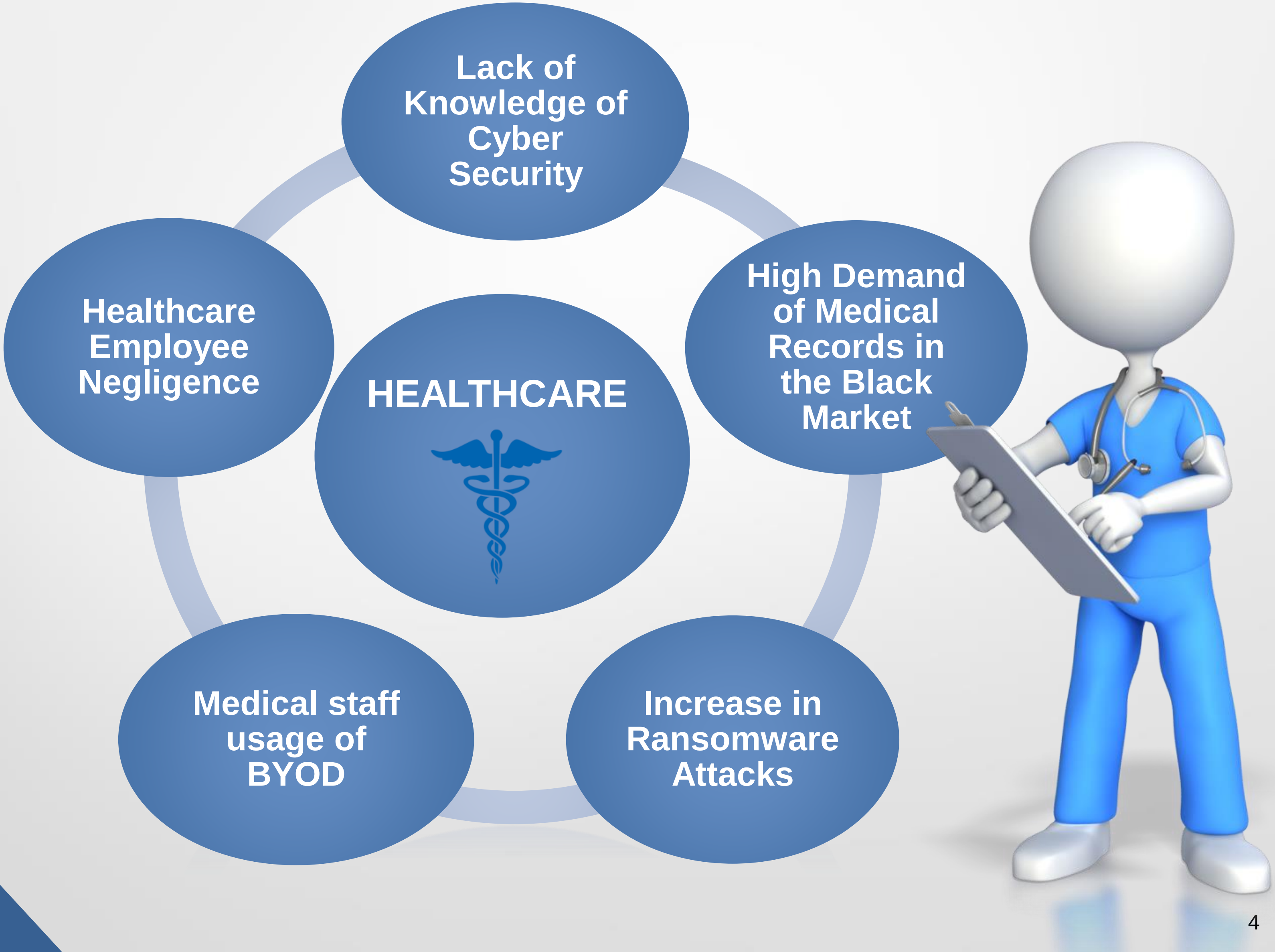
By industry classification, 2017 ($)

Total Internet Devices	IoT Devices	Global Population
20 Billion	› 8.4 Billion	› 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

CYBER RISK IN HEALTHCARE



Lack of Knowledge of Cyber Security

High Demand of Medical Records in the Black Market

Increase in Ransomware Attacks

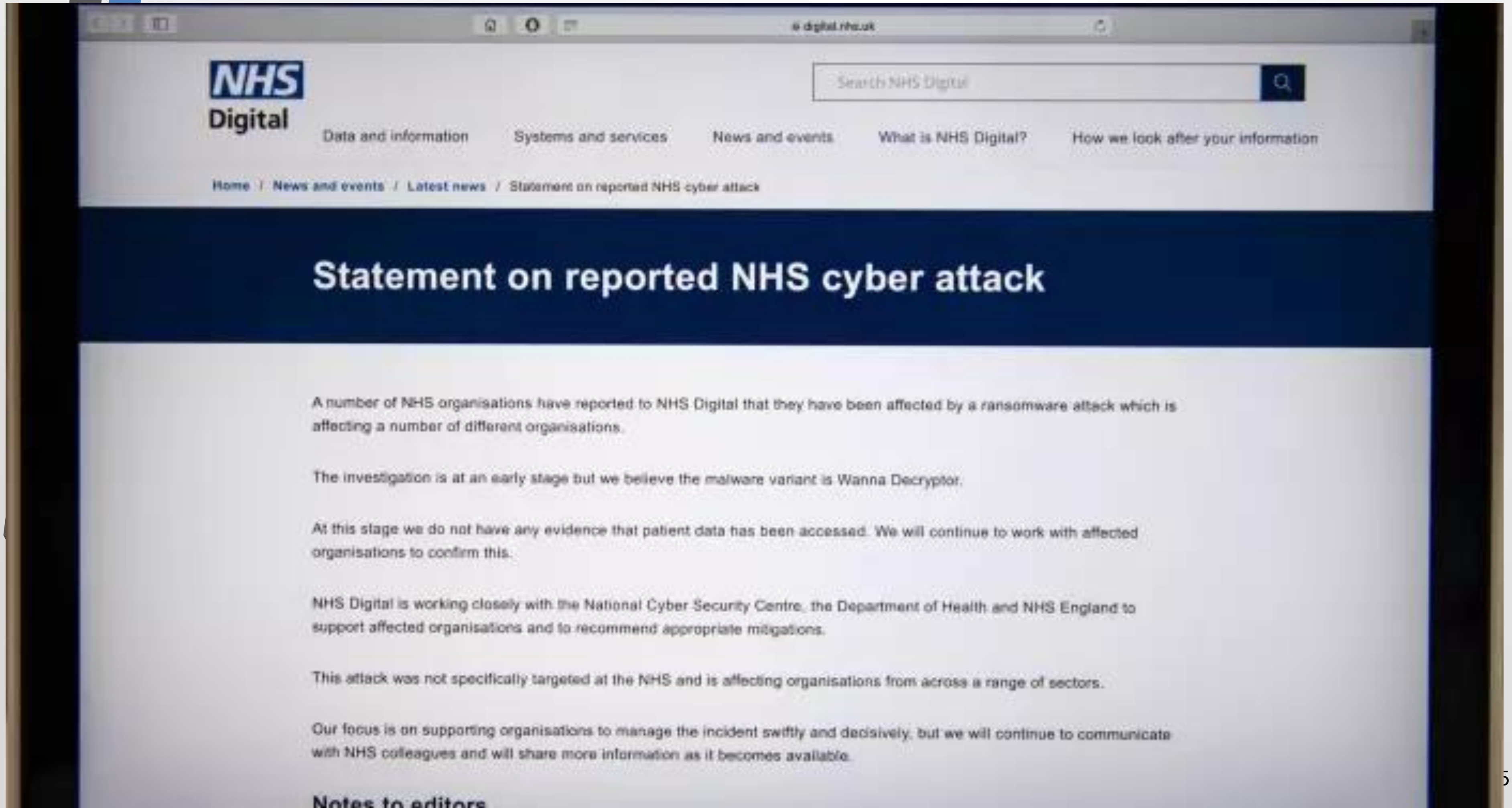
Medical staff usage of BYOD

Healthcare Employee Negligence

HEALTHCARE

WannaCry

May 12, 2017



Statement on reported NHS cyber attack

A number of NHS organisations have reported to NHS Digital that they have been affected by a ransomware attack which is affecting a number of different organisations.

The investigation is at an early stage but we believe the malware variant is Wanna Decryptor.

At this stage we do not have any evidence that patient data has been accessed. We will continue to work with affected organisations to confirm this.

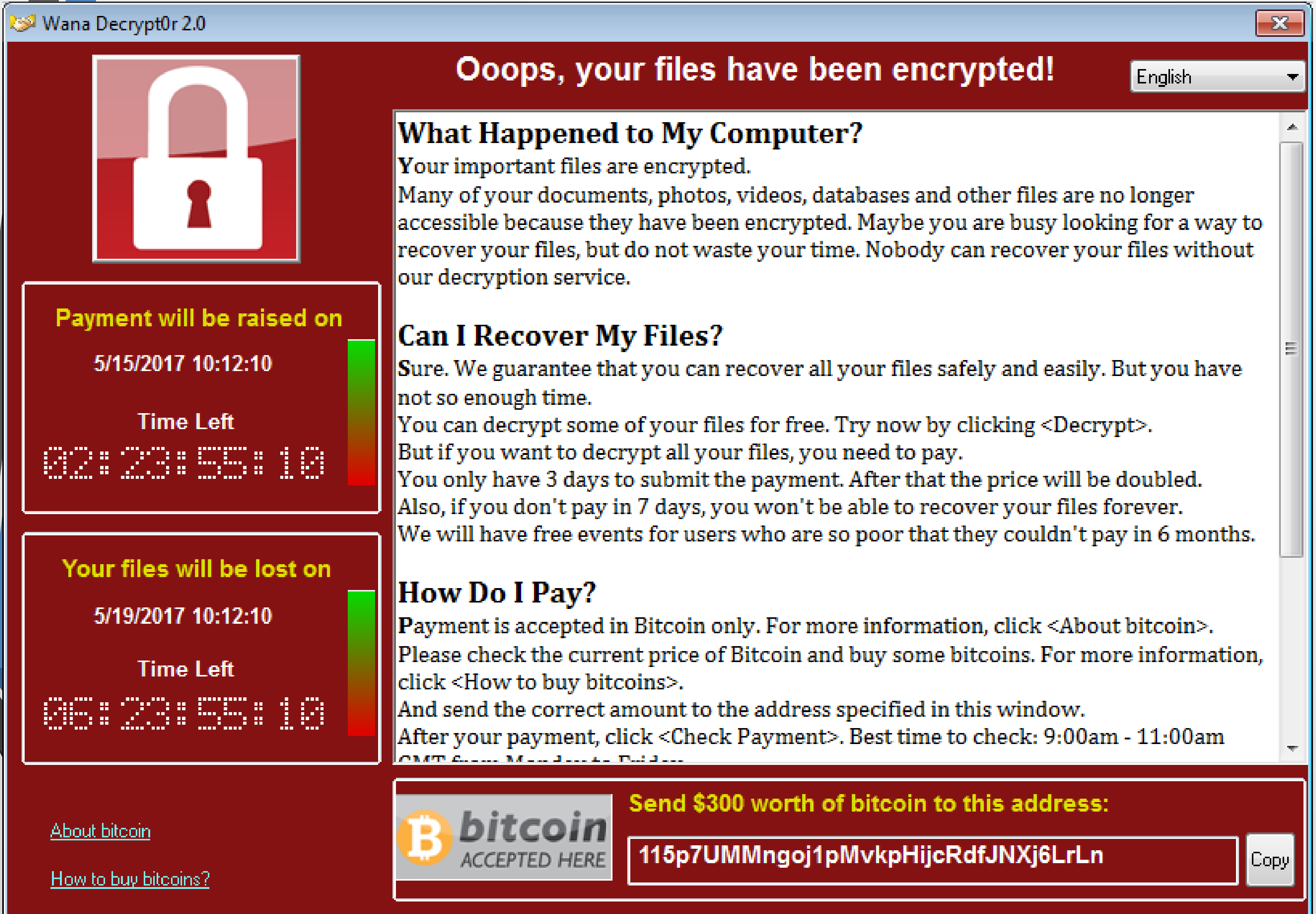
NHS Digital is working closely with the National Cyber Security Centre, the Department of Health and NHS England to support affected organisations and to recommend appropriate mitigations.

This attack was not specifically targeted at the NHS and is affecting organisations from across a range of sectors.

Our focus is on supporting organisations to manage the incident swiftly and decisively, but we will continue to communicate with NHS colleagues and will share more information as it becomes available.

Notes to editors

WannaCry



Ooops, your files have been encrypted!

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

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.

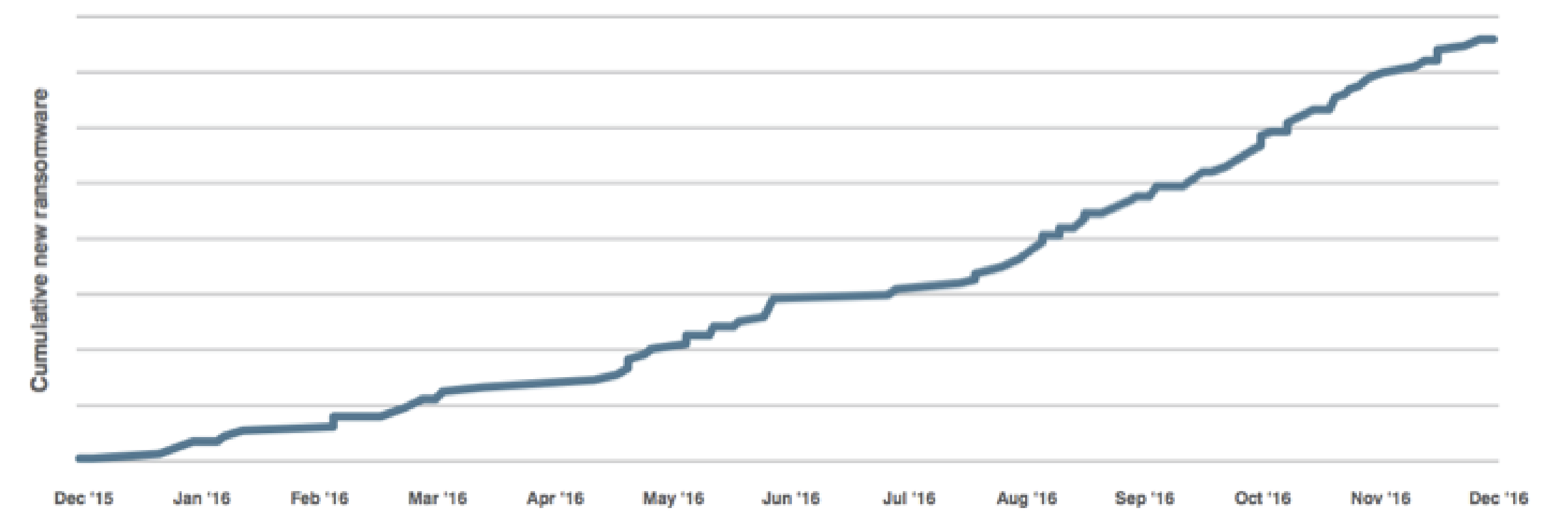
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Ransomware Attacks are Pervasive

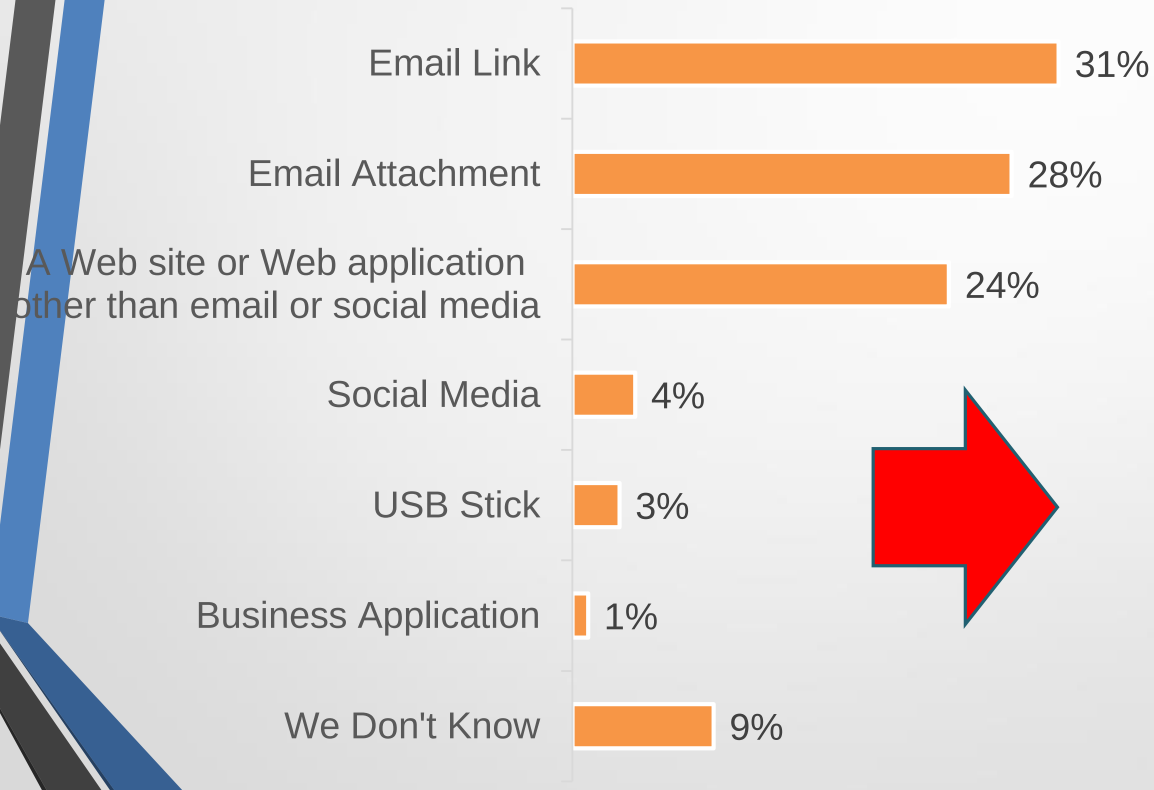
Ransomware Variants Grew by 30x in 2016

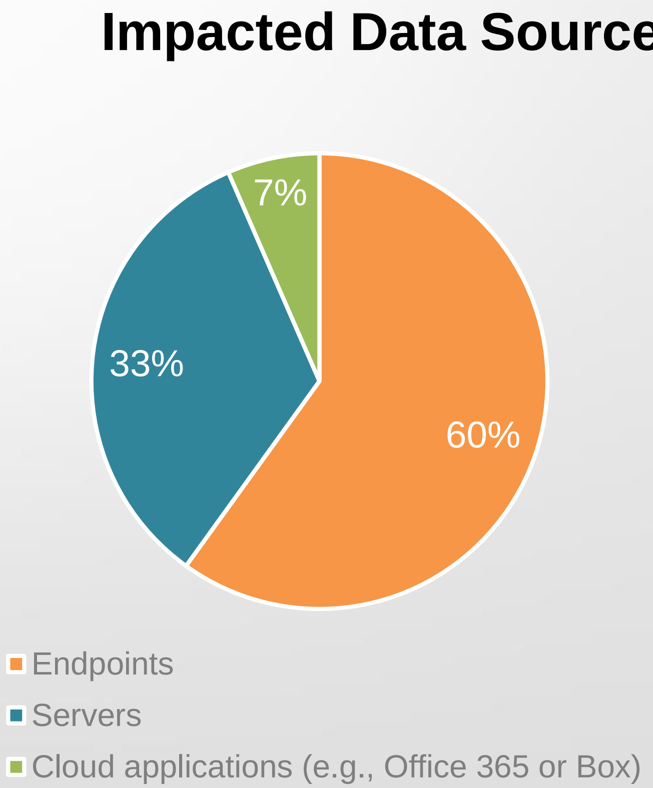


- A company gets hit every 40 seconds
- 50% of organizations attacked by ransomware are hit more than once
- Phishing email attachments are the #1 delivery vehicle

Source:
Proofpoint (https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-final-cm.pdf)
Barkly: https://blog.barkly.com/new-ransomware-trends-2017

Ransomware Vectors

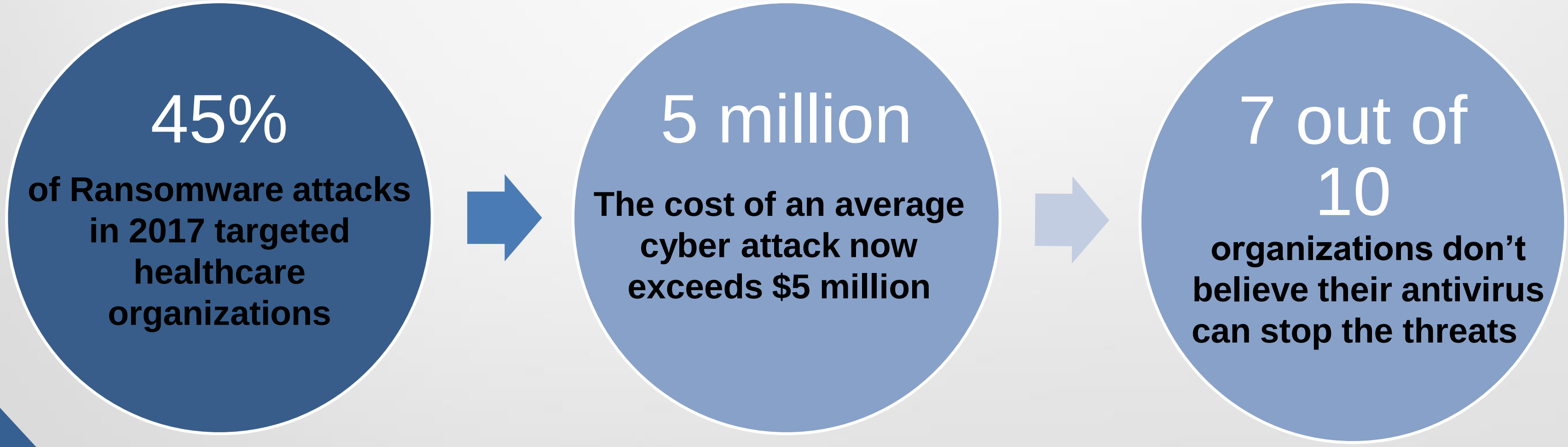




Source:
Proofpoint (https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-final-cm.pdf)
Barkly: https://blog.barkly.com/new-ransomware-trends-2017

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

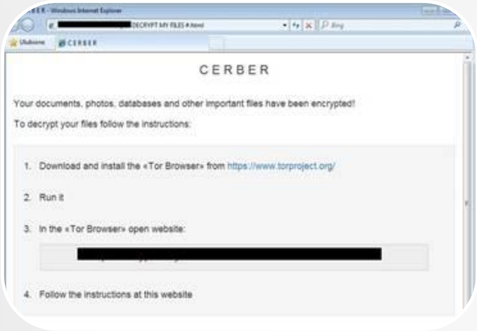
5 million

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 - Windows Internet Explorer

[redacted] DECRYPT MY FILES #.html

CERBER

Your documents, photos, databases and other important files have been encrypted!

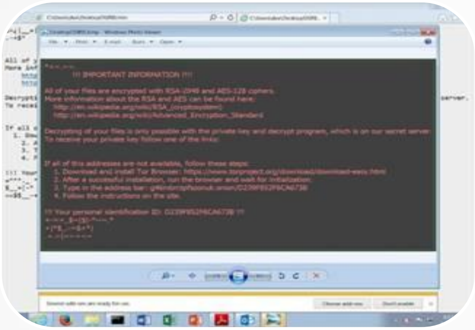
To decrypt your files follow the instructions:

1. Download and install the «Tor Browser» from https://www.torproject.org/
2. Run it
3. In the «Tor Browser» open website:

   [redacted]

4. Follow the instructions at this website

Cerber



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

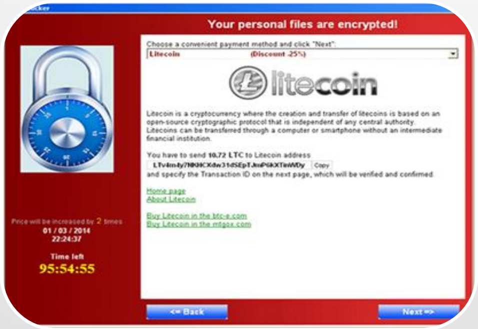
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [illegible].onion/D239F652F6CA6738
4. Follow the instructions on the site.

!!! Your personal identification ID: D239F652F6CA6738 !!!

Locky

SamSam Ransomware Attack Exploiting
Organization Network Vulnerabilities
PRESS ANY KEY!

Samsam



Your personal files are encrypted!

Choose a convenient payment method and click "Next":

Litecoin (Discount -25%)

Litecoin is a cryptocurrency where the creation and transfer of litecoins is based on an open-source cryptographic protocol that is independent of any central authority. Litecoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **10.72 LTC** to Litecoin address
LTv4m4y7HKHCXdw31dSEpTJmP6KXTmWDy Copy
and specify the Transaction ID on the next page, which will be verified and confirmed.

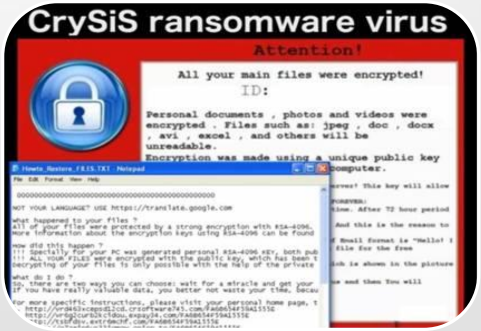
Home page
About Litecoin

Buy Litecoin in the btc-e.com
Buy Litecoin in the mtgox.com

Price will be increased by 2 times
01 / 03 / 2014
22:24:37

Time left
95:54:55

Cryptowall



Attention!

All your main files were encrypted!
ID:

Personal documents , photos and videos were encrypted . Files such as: jpeg , doc , docx , avi , excel , and others will be unreadable.
Encryption was made using a unique public key
computer.
server! This key will allow
FOREVER:
time. After 72 hour period
And this is the reason to
Email format is "Hello! I
file for the free
which is shown in the picture
e and then You will

Howto_Restore_FILES.TXT - Notepad

```
 0000000000000000000000000000000000000000000000
NOT YOUR LANGUAGE? USE https://translate.google.com

what happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both pub
!!! ALL YOUR FILES were encrypted with the public key, which has been t
Decrypting of your files is only possible with the help of the private

what do I do ?
So, there are two ways you can choose: wait for a miracle and get your
If you have really valuable data, you better not waste your time, becau

For more specific instructions, please visit your personal home page, t
  http://vrd463xcepsd12cd.crsoftware745.com/FA6B654F59A1555E
  http://vr6g2curb2kc1dou.expay34.com/FA6B654F59A1555E
  http://tsbfdsv.extr6mchf.com/FA6B654F59A1555E
```

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

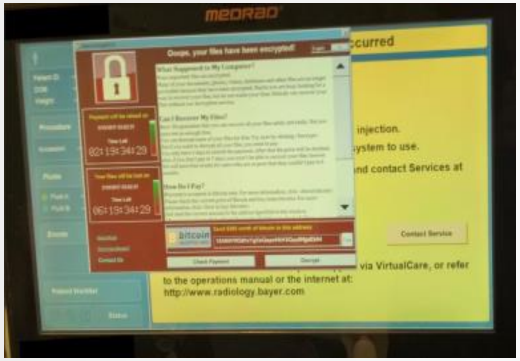
Only 42%

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



Ooops, your files have been encrypted!

ccurred

injection.

ystem to use.

nd contact Services at

via VirtualCare, or refer to the operations manual or the internet at: http://www.radiology.bayer.com

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

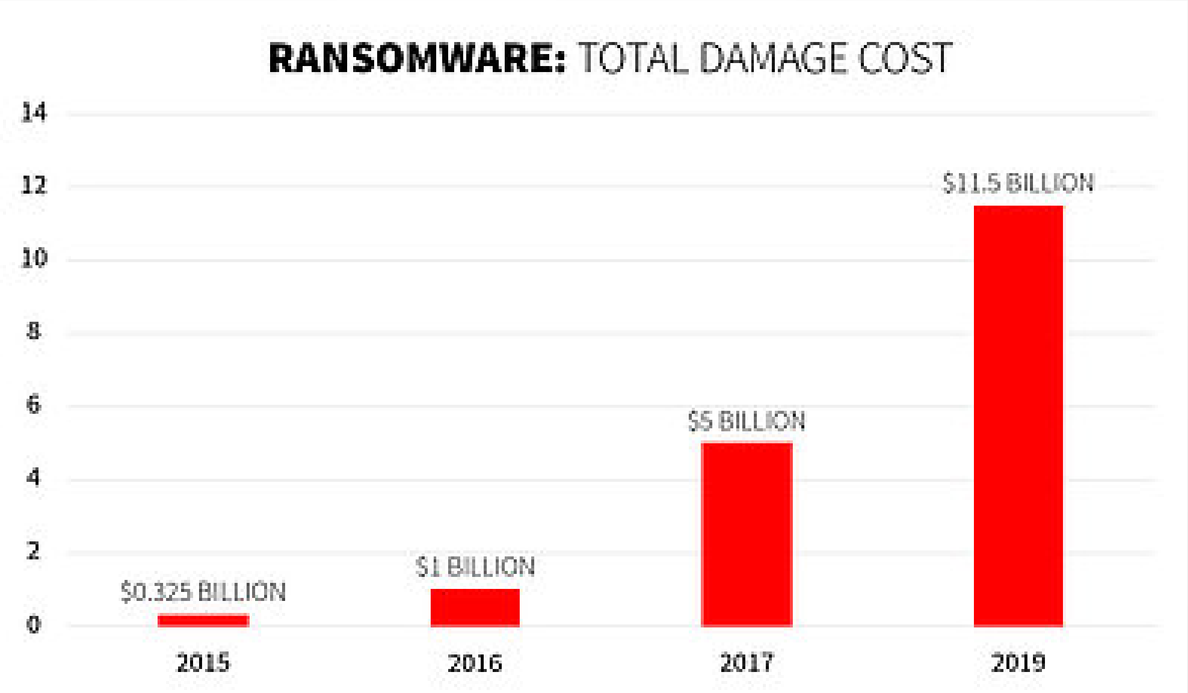
- The California-based Center for Orthopedic Specialists (COS) is notifying 85,000 of its current and former patients that a ransomware attack on its IT vendor may have breached their data.

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



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 disconnected (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

Use Endpoint Protection

Recovery Disaster Plan

Employee Training

Invest in a Cybersecurity Program

Block Unknown Users

GPO Restrictions

Q & A

CONTACT INFORMATION

(844) 55-CYBER (29237)

Sanjay.Deo@24by7security.com

Contact@24by7security.com

www.24By7Security.com

@24By7Security