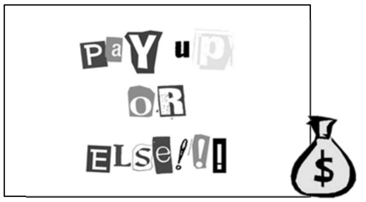
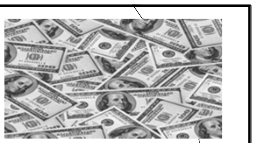


RANSOMWARE: SHOULD I NOTIFY LAW ENFORCEMENT?

Common Definitions



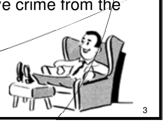
Ransom: “A consideration paid or demanded for the release of someone or something from captivity.” www.merriam-webster.com/dictionary/ransom

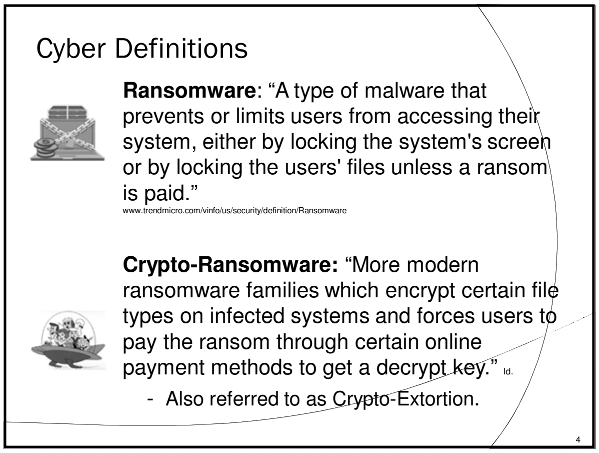
Extortion: “Obtaining money or property by threat or force.” criminal.findlaw.com/criminal-charges/extortion.html

Everything Old is New Again

- Criminals engaged in these illegal activities long before the internet existed
  - Middle Ages knight warfare
  - Pirates
  - Salzburg-Bavaria 30 Years War
  - Kidnapping

- The internet provided a new venue for crime – a networked world of computers
  - Criminals can now commit an extremely lucrative crime from the comfort of their own home
  - $10 million to $50 million MONTHLY income for cybercriminals



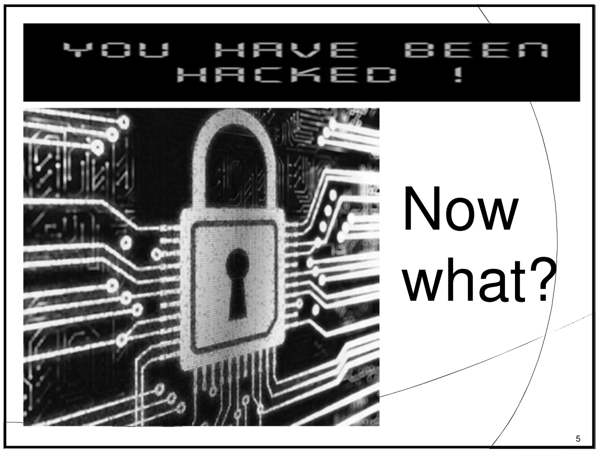


Cyber Definitions

Ransomware: “A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.”
www.trendmicro.com/vinfo/us/security/definition/Ransomware

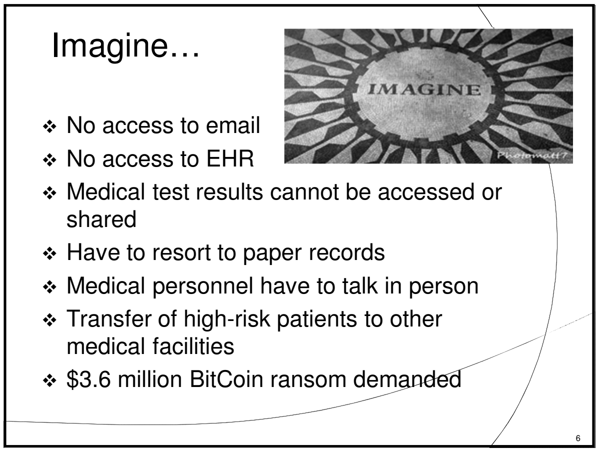
Crypto-Ransomware: “More modern ransomware families which encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.” Id.

- Also referred to as Crypto-Extortion.



YOU HAVE BEEN HACKED !

Now what?



Imagine…

- ❖ No access to email
- ❖ No access to EHR
- ❖ Medical test results cannot be accessed or shared
- ❖ Have to resort to paper records
- ❖ Medical personnel have to talk in person
- ❖ Transfer of high-risk patients to other medical facilities
- ❖ $3.6 million BitCoin ransom demanded

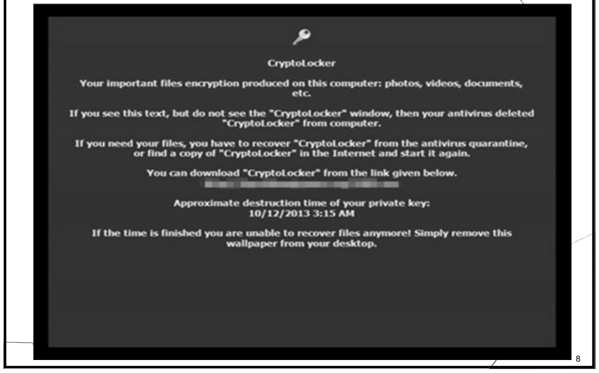
This is exactly what happened to Hollywood Presbyterian Medical Center in Los Angeles

Loss per day on CT Scans alone: $100,000

Ransom paid to decrypt files: $ 17,000

7

The threat



CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

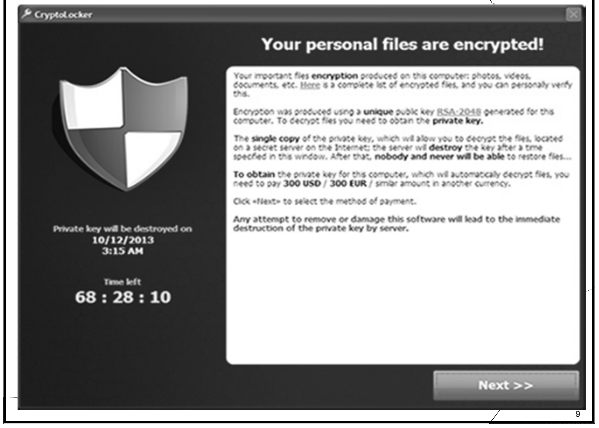
You can download "CryptoLocker" from the link given below.

[redacted]

Approximate destruction time of your private key:
10/12/2013 3:15 AM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

8



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

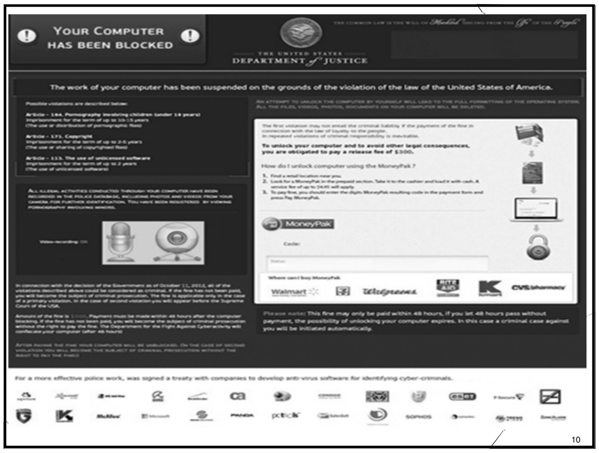
Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/12/2013
3:15 AM

Time left
68 : 28 : 10

9



YOUR COMPUTER HAS BEEN BLOCKED

THE UNITED STATES DEPARTMENT of JUSTICE

The common law is the will of Mankind issuing from the life of the People

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article - 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article - 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article - 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

Video recording: ON

In connection with the decision of the Government as of October 11, 2012, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the Supreme Court of the USA.

Amount of the fine is $300. Payment must be made within 48 hours after the computer blocking. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer (after 48 hours)

AFTER PAYING THE FINE YOUR COMPUTER WILL BE UNBLOCKED. (IN THE CASE OF SECOND VIOLATION YOU WILL BECOME THE SUBJECT OF CRIMINAL PROSECUTION WITHOUT THE RIGHT TO PAY THE FINE)

AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF THE OPERATING SYSTEM. ALL THE FILES, VIDEOS, PHOTOS, DOCUMENTS ON YOUR COMPUTER WILL BE DELETED.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people.
In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300.

How do I unlock computer using the MoneyPak ?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

MoneyPak

Code:

Status:

Where can I buy MoneyPak

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires. In this case a criminal case against you will be initiated automatically.

For a more effective police work, was signed a treaty with companies to develop anti-virus software for identifying cyber-criminals.

The Risk

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016.

This represents a 300% increase over the 1,000 daily ransomware attacks reported in 2015.

Source: How to Protect Your Networks from Ransomware, US Government Interagency Technical Guidance Document file://data_new01/Horizon/UserData/warrenr/My%20Documents/Healthcare/Ransomware/technical-document-ransomware-prevention-and-response.pdf

The Cost

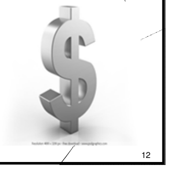
MONETARY

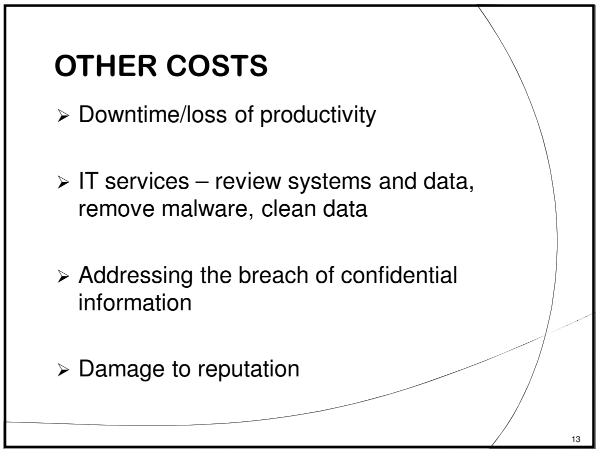
2015 - FBI's Internet Crime Complaint Center (IC3) received 2400 ransomware reports

Losses = $24 million
Average Ransom demand: $10,000

First Quarter 2016

Ransom Cost: $209 million
FBI's forecast for 2016 losses = $1 billion

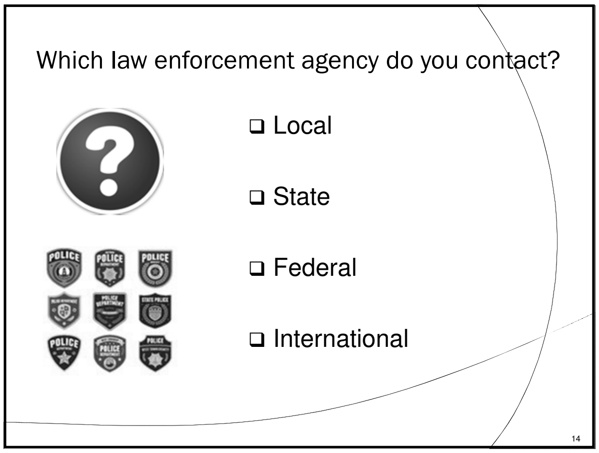




OTHER COSTS

- ➢ Downtime/loss of productivity
- ➢ IT services – review systems and data, remove malware, clean data
- ➢ Addressing the breach of confidential information
- ➢ Damage to reputation

13



Which law enforcement agency do you contact?

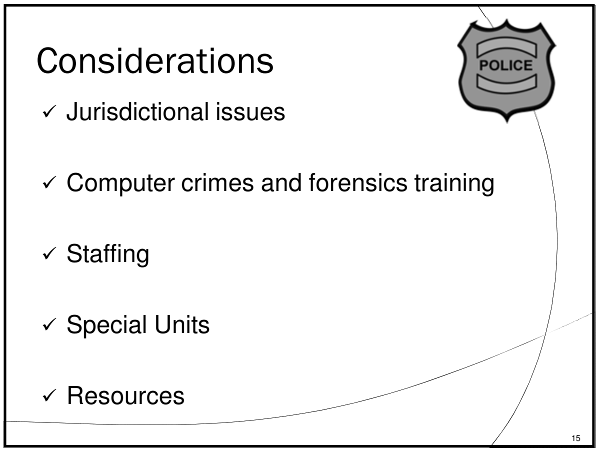
❑ Local

❑ State

❑ Federal

❑ International

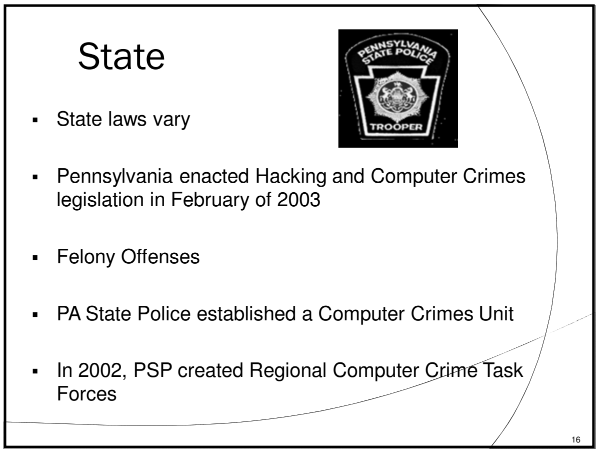
14



Considerations

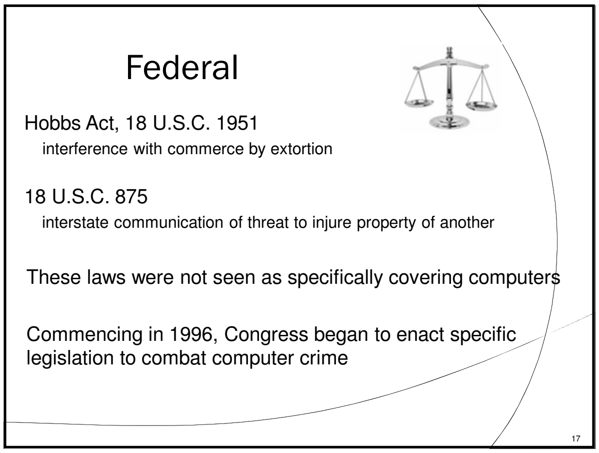
- ✓ Jurisdictional issues
- ✓ Computer crimes and forensics training
- ✓ Staffing
- ✓ Special Units
- ✓ Resources

15



State

- State laws vary
- Pennsylvania enacted Hacking and Computer Crimes legislation in February of 2003
- Felony Offenses
- PA State Police established a Computer Crimes Unit
- In 2002, PSP created Regional Computer Crime Task Forces



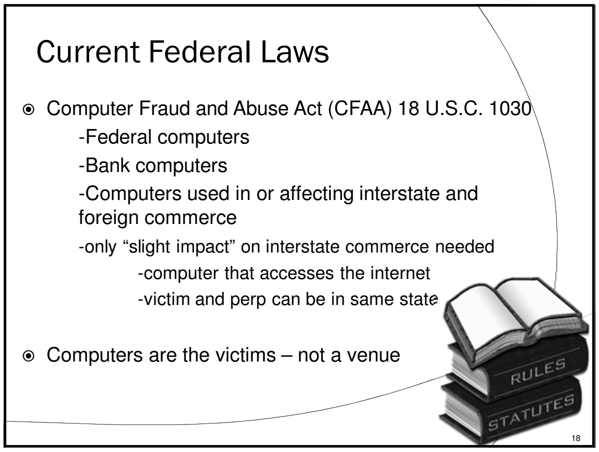
Federal

Hobbs Act, 18 U.S.C. 1951
interference with commerce by extortion

18 U.S.C. 875
interstate communication of threat to injure property of another

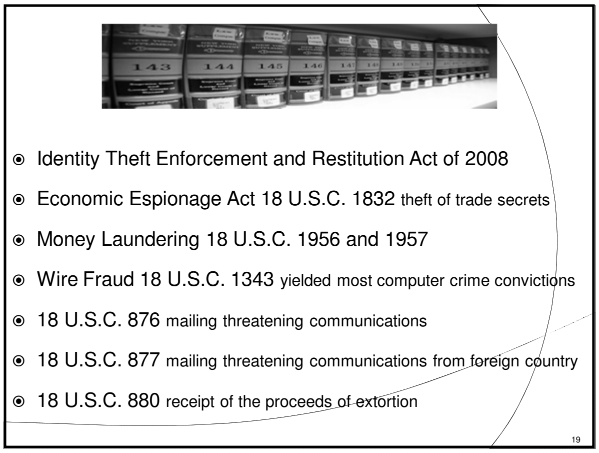
These laws were not seen as specifically covering computers

Commencing in 1996, Congress began to enact specific legislation to combat computer crime



Current Federal Laws

- Computer Fraud and Abuse Act (CFAA) 18 U.S.C. 1030
  - -Federal computers
  - -Bank computers
  - -Computers used in or affecting interstate and foreign commerce
  - -only “slight impact” on interstate commerce needed
    - -computer that accesses the internet
    - -victim and perp can be in same state
- Computers are the victims – not a venue

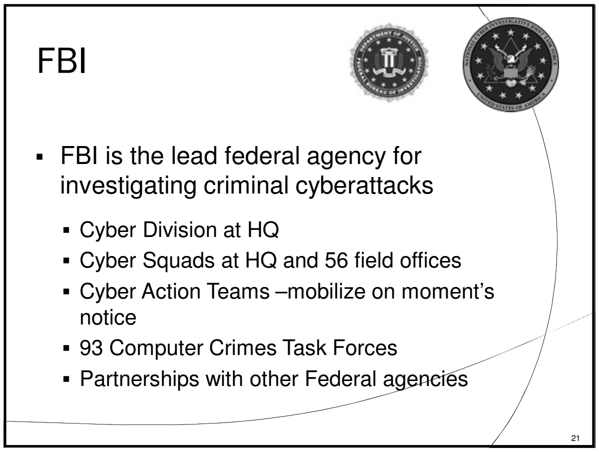


- Identity Theft Enforcement and Restitution Act of 2008
- Economic Espionage Act 18 U.S.C. 1832 theft of trade secrets
- Money Laundering 18 U.S.C. 1956 and 1957
- Wire Fraud 18 U.S.C. 1343 yielded most computer crime convictions
- 18 U.S.C. 876 mailing threatening communications
- 18 U.S.C. 877 mailing threatening communications from foreign country
- 18 U.S.C. 880 receipt of the proceeds of extortion

19

Federal Agencies

20

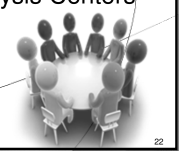


FBI

- FBI is the lead federal agency for investigating criminal cyberattacks
  - Cyber Division at HQ
  - Cyber Squads at HQ and 56 field offices
  - Cyber Action Teams –mobilize on moment’s notice
  - 93 Computer Crimes Task Forces
  - Partnerships with other Federal agencies

21

- Leads the National Cyber Investigative Joint Task Force (NCIJTF)
  - domestic coordination
  - established 2008
- National Cyber Forensics and Training Alliance (NCFTA)
- Partners with private sector through InfraGard and Information Sharing and Analysis Centers (ISACs)
  - 16 crucial infrastructure sectors
  - Includes healthcare and public health

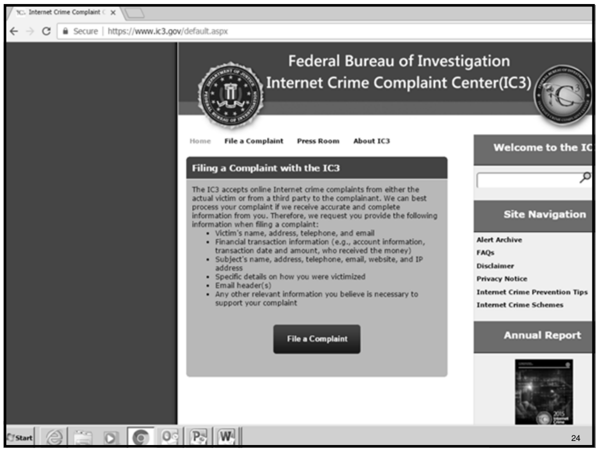


Internet Crime Complaint Center (IC3)

www.ic3.gov

FBI Internet Crime Complaint Center

Filing a Report



Internet Crime Complaint C ×
Secure | https://www.ic3.gov/default.aspx

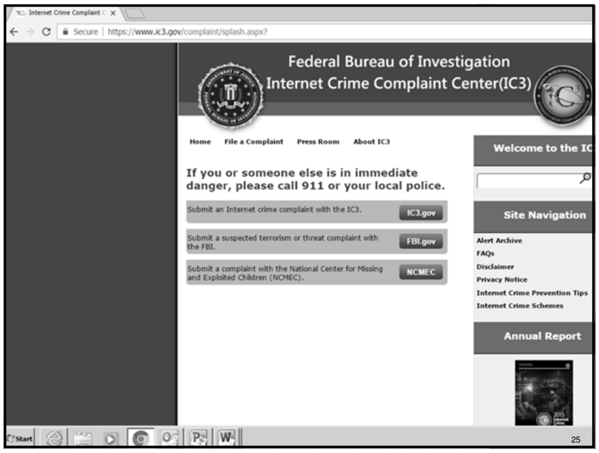
Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Home
File a Complaint
Press Room
About IC3
Welcome to the IC

Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint



Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

If you or someone else is in immediate danger, please call 911 or your local police.

Submit an Internet crime complaint with the IC3.

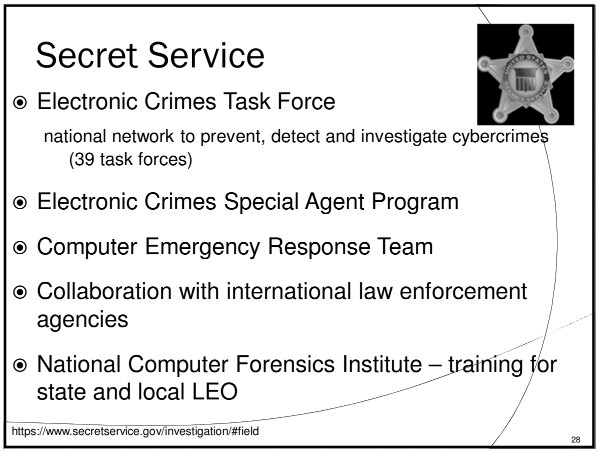
Submit a suspected terrorism or threat complaint with the FBI.

Submit a complaint with the National Center for Missing and Exploited Children (NCMEC).

Q: What details will I be asked to include in my complaint?

- Victim's name, address, telephone, email
- Financial transaction information
- Suspect's name, address, telephone, email, website, IP address
- Date and details on how you were victimized
- Initial entry vector or vulnerability if known
- How detected
- Specific assets impacted
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint

- Analysts review each report
- Refer to appropriate law enforcement agency for investigation and prosecution
- IC3 database shared through Law Enforcement Enterprise Portal (LEEP) – compare and compile
- Report cannot be withdrawn once submitted



Secret Service

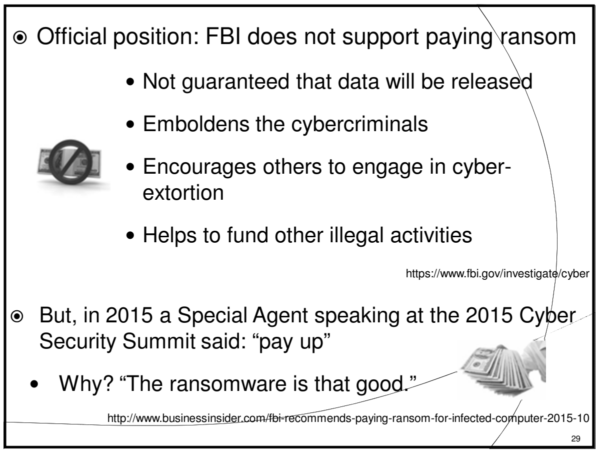
- Electronic Crimes Task Force

  national network to prevent, detect and investigate cybercrimes (39 task forces)

- Electronic Crimes Special Agent Program
- Computer Emergency Response Team
- Collaboration with international law enforcement agencies
- National Computer Forensics Institute – training for state and local LEO

https://www.secretservice.gov/investigation/#field

28



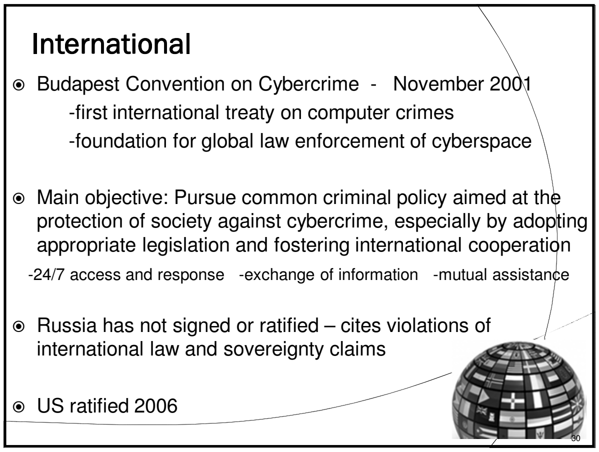
- Official position: FBI does not support paying ransom
  - Not guaranteed that data will be released
  - Emboldens the cybercriminals
  - Encourages others to engage in cyber-extortion
  - Helps to fund other illegal activities

https://www.fbi.gov/investigate/cyber

- But, in 2015 a Special Agent speaking at the 2015 Cyber Security Summit said: “pay up”
  - Why? “The ransomware is that good.”

http://www.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10

29



International

- Budapest Convention on Cybercrime - November 2001

  -first international treaty on computer crimes

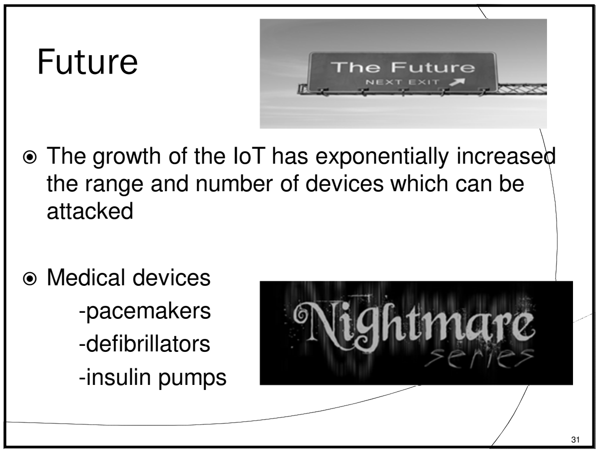
  -foundation for global law enforcement of cyberspace

- Main objective: Pursue common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation

  -24/7 access and response -exchange of information -mutual assistance

- Russia has not signed or ratified – cites violations of international law and sovereignty claims
- US ratified 2006

30

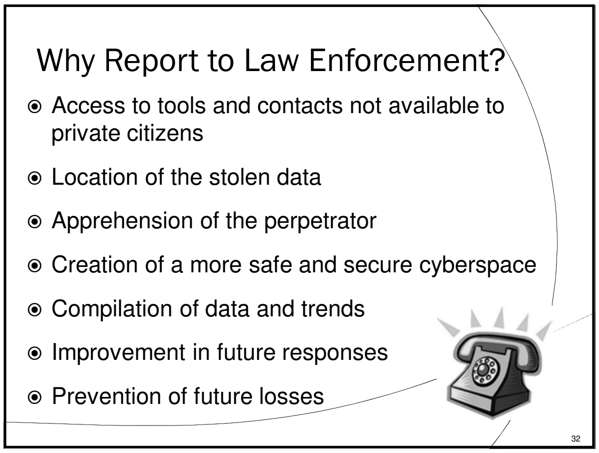


Future

- The growth of the IoT has exponentially increased the range and number of devices which can be attacked
- Medical devices
  - -pacemakers
  - -defibrillators
  - -insulin pumps

The Future
NEXT EXIT
Nightmare
series

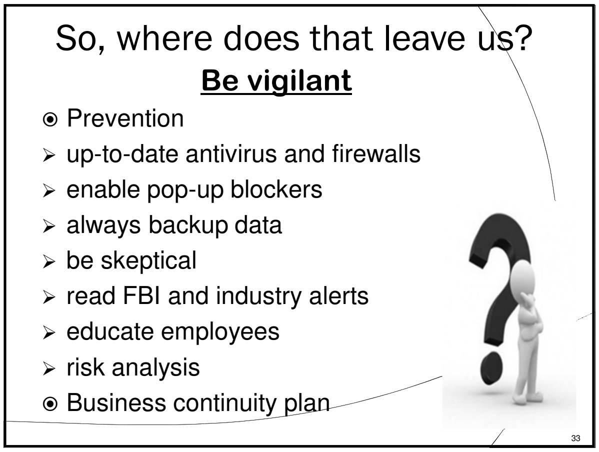
31



Why Report to Law Enforcement?

- Access to tools and contacts not available to private citizens
- Location of the stolen data
- Apprehension of the perpetrator
- Creation of a more safe and secure cyberspace
- Compilation of data and trends
- Improvement in future responses
- Prevention of future losses

32



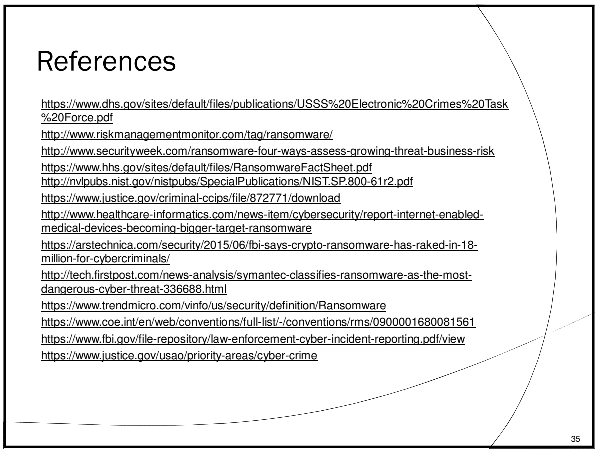
So, where does that leave us?

Be vigilant

- Prevention
- ➢ up-to-date antivirus and firewalls
- ➢ enable pop-up blockers
- ➢ always backup data
- ➢ be skeptical
- ➢ read FBI and industry alerts
- ➢ educate employees
- ➢ risk analysis
- Business continuity plan

33

Reporting helps law enforcement make cyberspace safer for everyone



References

https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf

http://www.riskmanagementmonitor.com/tag/ransomware/

http://www.securityweek.com/ransomware-four-ways-assess-growing-threat-business-risk

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://www.justice.gov/criminal-ccips/file/872771/download

http://www.healthcare-informatics.com/news-item/cybersecurity/report-internet-enabled-medical-devices-becoming-bigger-target-ransomware

https://arstechnica.com/security/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/

http://tech.firstpost.com/news-analysis/symantec-classifies-ransomware-as-the-most-dangerous-cyber-threat-336688.html

https://www.trendmicro.com/vinfo/us/security/definition/Ransomware

https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view

https://www.justice.gov/usao/priority-areas/cyber-crime