CyberCon Africa

Richard C. LaMagna CPP CISM
NW3C - Global Trust Group

October 16-17, 2017

“We believe that data … is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – **then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world.**“
(Ginni Rometty IBM Chairman and CEO, New York City Security Summit 2017)

Main Messages

- Cybersecurity is not solely a technical issue and technology is not the primary solution: people are the weakest link.
- Sharing threat intelligence is the only way to be proactive in a constantly changing cyber threat environment.
- Cyber crime must be addressed through cooperation on a global basis
- Public- Private Partnerships (PPPs) are key to cooperation

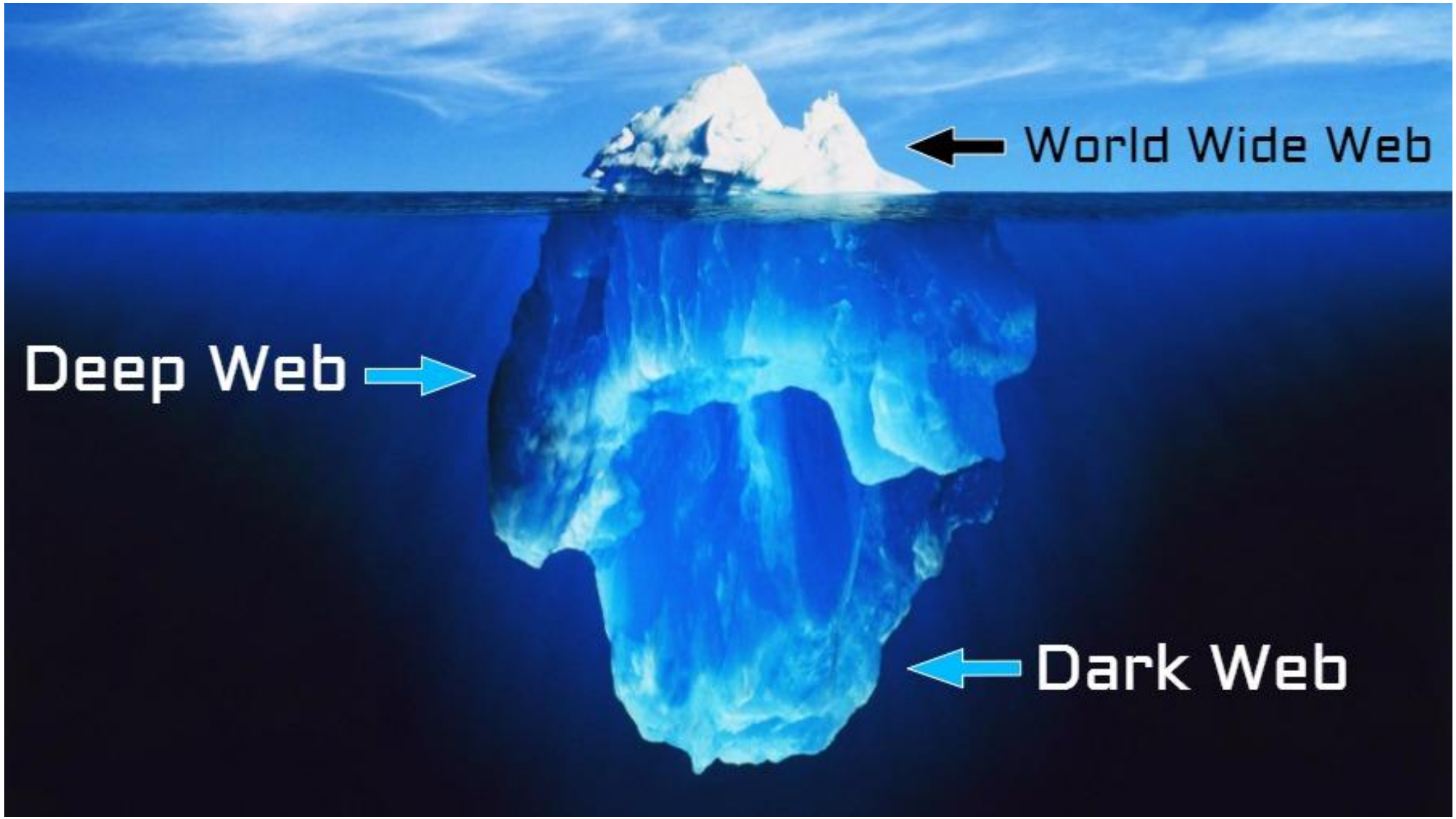
Types of Cybercrime

- Intrusions/ breaches of personal or corporate privacy
- Use of illegally obtained digital information for blackmail or extortion
- Identity theft
- Transaction-based crimes such as fraud, ransom and drug trafficking
- Trafficking in child pornography, women and children
- Digital piracy, money laundering, and counterfeiting
- Altering data or defacing web sites for profit or political objectives
- Electronic harassment

Global Cybercrime

- Average time to detect a cyber attack is **205 days**[2]
- Average time to resolve incident **45 days**
- Average cost per cyber incident to large companies **$1.6 M**
- Huge financial incentives for hackers to get personally identifiable information, bank account and credit card data; buy and sell it on the **Dark Web**
- **Dark Web -** anonymity through **TOR** browser and proxy servers
- **Eighty-nine (89) percent** of breaches in 2015 had a financial or espionage motive. (Verizon Data Breach Report 2016)

[1] Cybersecurity Venture's 2016 Cybercrime Report [2]Gartner


World Wide Web
Deep Web
Dark Web

Global Cybercrime Trends

- Economic damage caused by cybercrime will increase from $3 Trillion in 2015 to $6Tglobally by 2021[1] estimate based on: (WW Economic Forum)

  - Year-over-year growth
  - Dramatic increase in state-sponsored attacks
  - Organized crime hacking
  - Greater cyber-attack surfaces

[1] Cybersecurity Venture's 2016 Cybercrime Report

Explosion in Ransomware Attacks

- Every 40 seconds a business is victim of a ransomware attack
- For individuals, it's every 10 seconds
- 1/5 SMBs that paid ransom never got data back
- **Mobile Ransomware attacks in 2017 up 250% in Q1[1]**
- **No More Ransom** project launched July 2016- cooperation amongst Police, EUROPOL, McAfee, and Kaspersky Lab…free online decryption tools[1] https:// www.nomoreransom.org

[1] Tech Republic May 22, 2017 , www.techrepublic.com; Securelist Kaspersky Security Bulletin 2016;The Ransomware Revolution. https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/

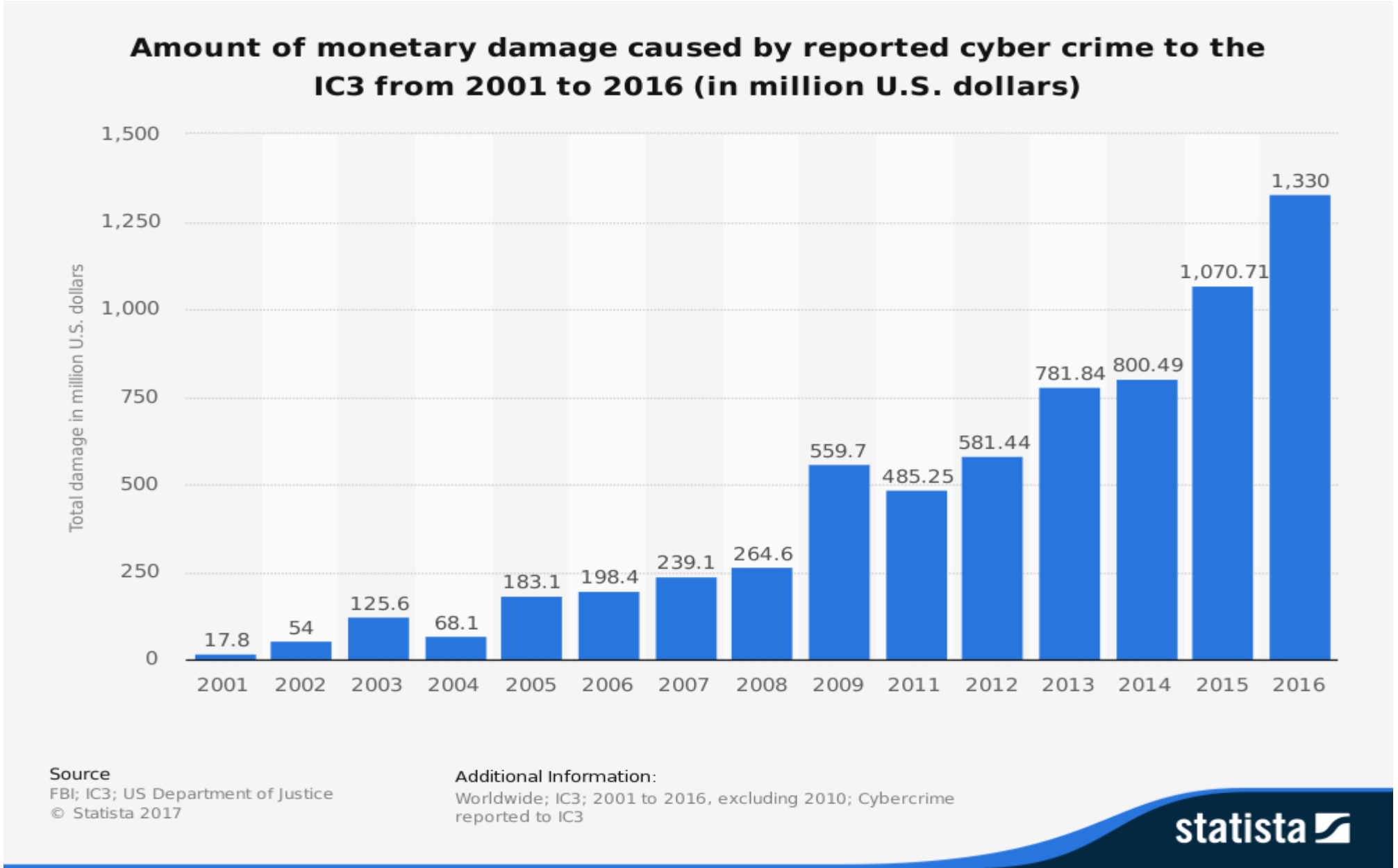
Cybercrime Trends- Internet of Things (IoT)

- Rapid increase in Internet connected devices e.g. smart phones, tablets, Industrial Control Systems, etc.
- IoT is causing new threats to emerge and increase; greater attack surfae
- Devices not meant to be Internet-enabled are online and vulnerable to attack-- networks are more vulnerable than ever because IoT devices offer new entry points for intrusions, e.g. webcam, HVAC, cars, etc.
- **Security awareness** is an issue-difficult enough to get people to think about PC and mobile device security—now it’s IoT, every day devices like thermostats, refrigerators, etc. are not secured and vulnerable

Who are the attackers ?

- **Hacktivists** (Hacker-Activists): politically or ideologically motivated to deface websites, blogs and other digital media; launch DDoS (distributed denial of service) attacks
- **Insiders Threats:** employees or contractors, who hack internal systems and data belonging to their employers, or behave carelessly and ignore security rules
- **Cyber-Gangs:** groups of hackers sponsored by criminal organizations; illegal hacking to steal large sums of money, commit extortion and other crimes.
- **Cyber-Spies:** (often state-sponsored) commit espionage through digital surveillance, and theft of confidential data e.g. government and trade secrets,
- **Cyber-Terrorists:** use technology to commit cyber-attacks which harm people, places and things
- **Cyber-Criminals:** any of the above, hackers who use technology and social engineering against organizations and individuals for financial gain, notoriety, or both

FBI's Internet Crime Complaint Center (IC3)



Top Cyber Attacks in 2017

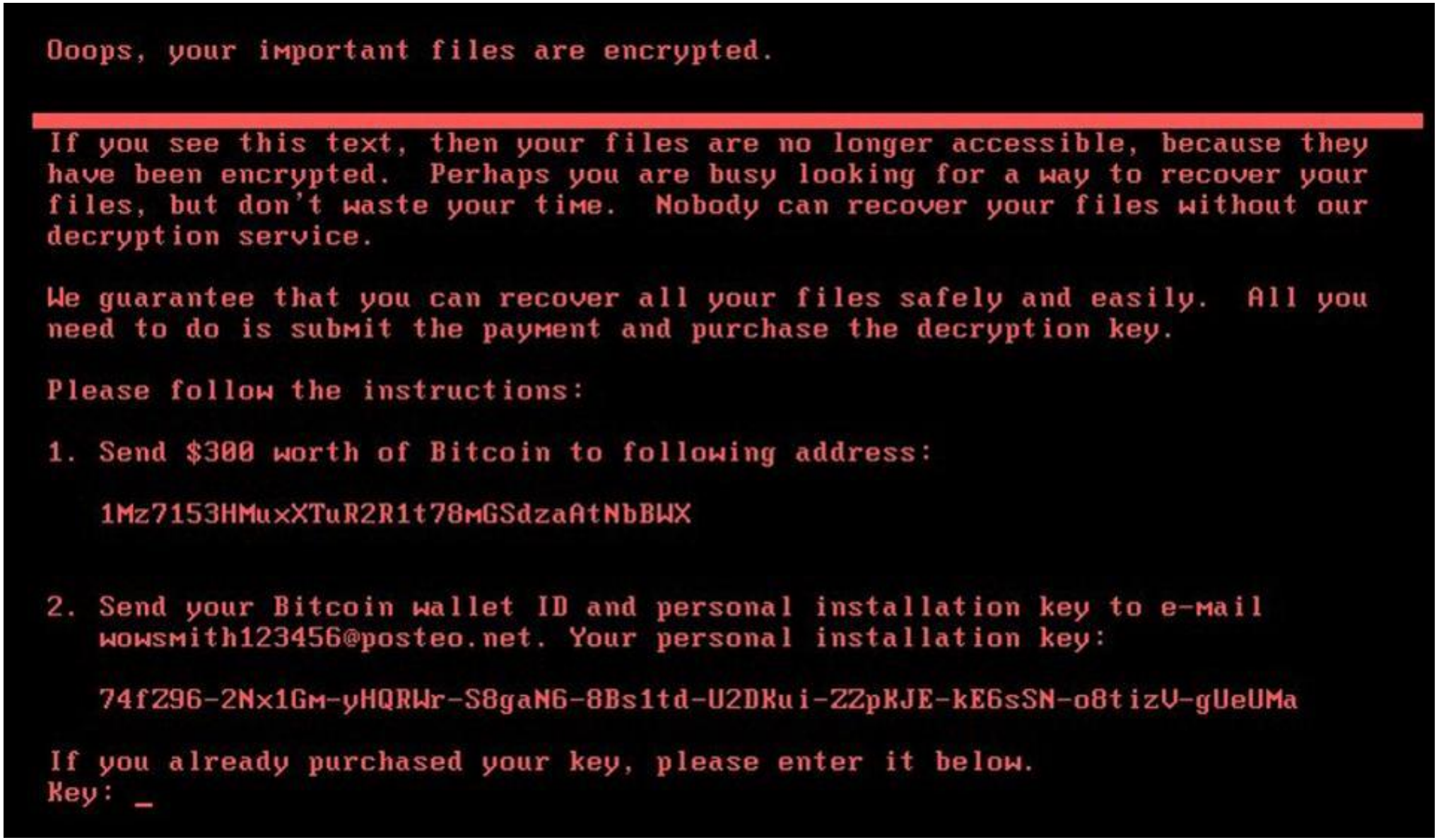
- **Shadow Brokers**- hacking group claimed to have breached NSA Operation Equation; leaked NSA tools including Windows exploit

- **Wannacry Ransomware**-attacked hundreds of thousand of targets, public utilities, large corporations, hospitals in 150 countries. Exploited security flaw in Windows XP; experts found “kill switch” to stop it—probably North Korean origin

- **Petya/Not Petya**- June 2017 massive outbreak of attacks across Europe and U.S. infected networks in multiple countries: Maersk shipping, Russian Oil Co. ,Chernobyl radiation detection systems; possibly intended to mask attack on Ukraine, disrupted power companies, Kiev Metro airports, transit, central bank, etc.

How the Equifax data breach happened: What we know now by Jackie Wattles and Selena Larson @CNNTech September 16, 2017, http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Petya Ransomware Screen Message



Top Cyber Attacks in 2017

- **Equifax-** large U.S. credit reporting agency; cyberattack that potentially exposed personal info of **143 million people**: names, social security numbers, addresses, driver's license numbers, etc.

- U.S. Department of Homeland Security, US-CERT, "identified and disclosed" the Apache Struts flaw in March, Equifax said they discovered it July 29.[1]

- Equifax CEO just resigned

How the Equifax data breach happened: What we know now by Jackie Wattles and Selena Larson @CNNTech September 16, 2017, http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Cybercrime in Africa

“Cybercrime accounts for losses of 1 billion Rand ($64 billion) for South Africa every year.” (0.14 % of GDP)

South African Banking Risk Information Centre (SABRIC)

Cybercrime in Africa

- Hundreds of millions of cyber attacks every year in Africa
- Banks and offices targeted by hackers with increasing frequency
- South Africa, Nigeria and Kenya most affected
- 70% of South Africans impacted by Cybercrime (world average 50%)[1]
- Cybercrime cost the South African economy an estimated $573 M; Nigerian economy $500 M; Kenyan economy$36 M per year[2]

[1]Cybercrime in Africa Facts & Figures , Zhudifeng, SCIDEVNet ;http://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html; [2] International Data Group Connect

Cyber Threat Vectors

- **Espionage-**The cyber war has already begun; state-sponsored hackers are stealing trade secrets at an unprecedented level

- **Industrial Control Systems**-legacy supervisory control and data acquisition (SCADA) networks;control critical infrastructure: electricity grids, natural gas, water, etc. not designed with security and are extremely vulnerable

- **Internet of things (IOT)**-the proliferation of connected devices from security cameras and monitoring systems to refrigerators, cars, and thermostats are vulnerable to Distributed Denial of Service (DDoS)attacks

Cyber Threat Vectors

- **Ransomware attacks-** rose 36% in 2017; attacks on large and small businesses, hospitals, schools and government agencies; now mainstream and a major source of revenue for criminals

- **Phishing attacks**- getting more sophisticated and targeted at key individuals within an organization; spear phishing email leads recipient to believe email is legitimate; **88 % of attacks** involved users opening a link[3]

- **Credential theft**– getting more common; no need for malicious code to break into a company's network; it's better to steal employees credentials or trick them into giving them; it's much harder to detect authorized user

[1] Symantec 2017 Internet Security Global Threat Report ,[2] RSA2017 Global Fraud and Cybercrime Forecast [3]Robert Steadman, Herjavec Grp. Cyber Report 2017

Critical Infrastructure Vulnerability: Cyberwarfare

- Hackers remain undetected for months in corporate and government networks —they access gateways to:
  - public utilities
  - nuclear power plants
  - transportation and air traffic control systems
  - world's money supply

- In December 2015 and 2016 Russian hackers attacked power grids in Ukraine, disrupted power for ¼ million people[1]; malware used in crippling Ukraine's power systems also affected mining and railway companies.

- Cyberwarfare underway; Estonia attacked by Russians in 2007; Iran attacked by US-Israel in Stuxnet malware attack June 2009-10.

[1]https://phys.org/news/2017-09-power-grid-circuit-simulation-methods.html

Challenges to Cybersecurity

- Threat detection and information sharing; criminals have anonymity
- Lack of security budgets
- Lack of international cooperation framework and public-private partnerships
- Not enough qualified cybersecurity personnel (One million Cybersecurity jobs open in 2016)[1]
- Lack of security awareness in general; careless online behavior
- Inadvertent insider breaches are growing; users open infected links
- End-user training was identified by 57% of respondents in survey as their leading method for combating threats[2]

[1]Cybersecurity Venture's 2016 Cybercrime Report

[2]The 2017 Threat Monitoring, Detection and Response Report by Cybersecurity Insiders

Solutions—People and Training Are Key

- End user security awareness training is fundamental to a cyber defense strategy -- employees are first line of defense against attacks
- Most hacking depends on social engineering e.g. spear phishing - employees are biggest vulnerability
- Minimizing the chance of attack through employee training is probably the single-most important thing to do
- Develop a culture of security in the organization-includes physical and cyber
- Stronger public-private partnerships to share threat information, informs prevention and preparedness

International Cooperation

Public Private Partnership Models

The **Council** of **Europe Convention** on **Cybercrime**

- Effective July 1, 2004- Canada, U.S. Japan and South Africa played key role in creation
- Russia, China, India and Brazil are not cooperative on grounds of sovereignty
- The **COE Convention** is first international treaty on crimes committed using the Internet and computer networks, dealing with infringements of copyright, computer-related fraud, child pornography and violations of network security
- Its main objective is to pursue a common criminal policy aimed at protecting society against cybercrime, by adopting appropriate legislation and fostering international cooperation
- Harmonization of laws and enhancing investigative techniques
- Recognized that cooperation has to be quick , provides for evidence preservation scheme through network of prosecutors and police officers working on 24/7 basis

Carnegie Mellon University **Computer Emergency Response Team (CERT)**

- Study and solve cybersecurity problems
- Identify vulnerabilities in software
- Develop tools, information and training to improve cybersecurity, etc.
- Contribute to long-term changes in networked systems
- Collaborate with high-level government organizations
- U.S. Department of Defense;Homeland Security (DHS)
- Law enforcement, e.g. FBI; the intelligence community; and many industry organizations.

Information Sharing and Analysis Centers (ISACs)

- Industry specific, e.g. Financial Services (FS-ISAC), Information Technology (IT-ISAC), Multi-state (MS-ISAC), Emergency Services (EMR-ISAC)
- National Council of ISACs (NCI) has 24 member ISACs that collaborate with each other through NCI
- ISACs help critical infrastructure owners and operators protect facilities, personnel and customers from cyber and physical security threats
- ISACs collect, analyze and disseminate actionable threat information to members and provide tools to mitigate risks and enhance resiliency

Financial Services (FS)-ISAC

- Mission: Share timely, relevant, actionable cyber and physical security information and analysis
- Designed, developed and owned by financial services industry, e.g. commercial banks, credit unions, major credit card and insurance companies, brokerage houses, etc.
- Shares information globally (7,000 members in 39 countries with user base in 72 countries)
- Publishes monthly brief for CEOs
- Communicates latest threat landscape in plain language

Information Sharing and Analysis Organizations (ISAOs)

- U.S. Pres. Executive Order in 2015 directed Dept. Homeland Security (DHS) to encourage development of ISAOs
- DHS-Nat'l Cybersecurity and Communications Center (NCCIC) coordinates and acts as clearing house for information sharing and analysis amongst government agencies and private sector partners
- ISAO Standards Organization set standards and ISAO operating guidelines that align with all industry groups, not just ISACs (primarily critical infrastructure)
- Standards are intended to be: **Voluntary, Transparent, Inclusive, Actionable** and **Flexible**

Cybersecurity Center of Excellence (CoE)

- COE does not duplicate existing capability, harmonizes and coordinates with existing entities and agencies
- COE is central point of coordination for specific needs of country; designed to provide support long-term as cybersecurity leader
- Harmonize and coordinate staff development in one location and coordinates information related to current cyber threats, perform cyber intelligence analytics, and incident response management training and policy
- Provides training to build technical operational capabilities that prevent and combat cyber threats and develops CISO leadership skills e.g. strategy formulation, PR, crisis management, etc.
- Host inter-agency and commercial sector meetings to increase collaboration and develop public-private partnerships

Resources

- Carnegie Mellon University, Software Engineering Inst. CERT http://www.cert.org/
- U.S. Department of Homeland Security :https://www.dhs.gov/topic/cybersecurity-information-sharing
- National Council of ISACs: https://www.nationalisacs.org/
- U.N. Office on Drugs and Crime (UNODC) https://www.unodc.org/
- European Cybercrime Centre-EC3- https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
- South Africa Portal for Cybercrime Resources: http://cybercrime.org.za/
- Rand Corp. Cybercrime: https://www.rand.org/topics/cybercrime.html
- Center for Internet Security: https://www.cisecurity.org/
- ISACA :https://www.isaca.org/pages/default.aspx
- Microsoft-https://www.microsoft.com/en-us/security/default.aspx?&WT.srch=1&wt.mc_id=AID623240_SEM_C9HtVpRB

Thank you

Questions or Comments ?