WORLD BANK GROUP

Cybersecurity in the Financial Sector

Aquiles A. Almansi
Lead Financial Sector Specialist
aalmansi@worldbank.org

WORLD BANK GROUP

More, more serious, incidents

- The average financial institution that IBM Security Services monitors worldwide experienced 65 percent more attacks than the average client across all industries in 2016, with a 29 percent increase from 2015.
- In the UK the number of cyber-attacks against financial services companies reported to the Financial Conduct Authority (FCA) rose by more than 80% in 2017.
- Some notorious incidents:
  - Central Bank of Bangladesh
  - Equifax
  - Several Mexican banks

WORLD BANK GROUP

Cyber exposure increasing

- Financial institutions and their customers keep quickly increasing their reliance on digital technologies. For example, according to PricewaterhouseCoopers, in the USA, 46 percent of bank customers were already digital-only in 2017, compared with 27 percent in 2012, and those customers interacting with bank staff continue to shrink, falling from 15 to 10 percent.

WORLD BANK GROUP

Regulatory response

- FSB: *Stocktake on Cybersecurity Regulatory and Supervisory Practices*

  http://www.fsb.org/wp-content/uploads/P131017-2.pdf

- World Bank-FinSAC: *Financial Sector's Cybersecurity: A Regulatory Digest*

  http://www.worldbank.org/finsac

- A. A. Almansi: *Financial Sector's Cybersecurity: Regulations and Supervision*

  http://documents.worldbank.org/curated/en/686891519282121021/pdf/1236655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

WORLD BANK GROUP

Regulatory response: key ideas

- Some jurisdictions approach cybersecurity and/or information technology risk explicitly, others address it implicitly as just one type of operational risk.

- Existing cybersecurity regulations typically address:
  - roles of the Board, Senior Management and, if present, the Chief Information Security Officer (CISO)
  - mandatory reporting of cyber/ICT incidents
  - outsourcing of ICT services

WORLD BANK GROUP

Regulatory response: other ideas

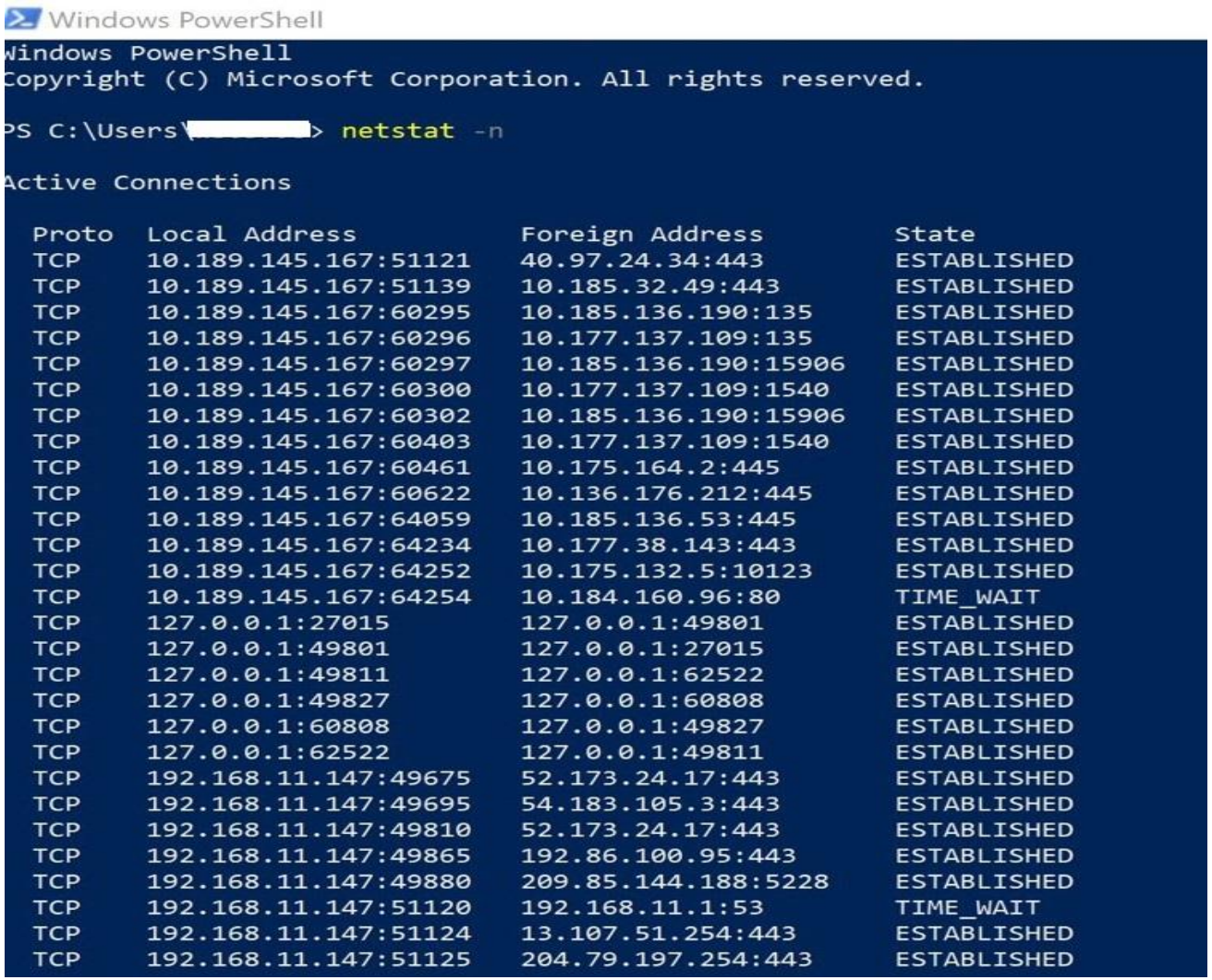
- Some regulations also address:
  - risk assessments
  - system access controls
  - incident response and recovery
  - simulations and testing
  - training
  - encryption protocols
  - etc., etc., ….

WORLD BANK GROUP

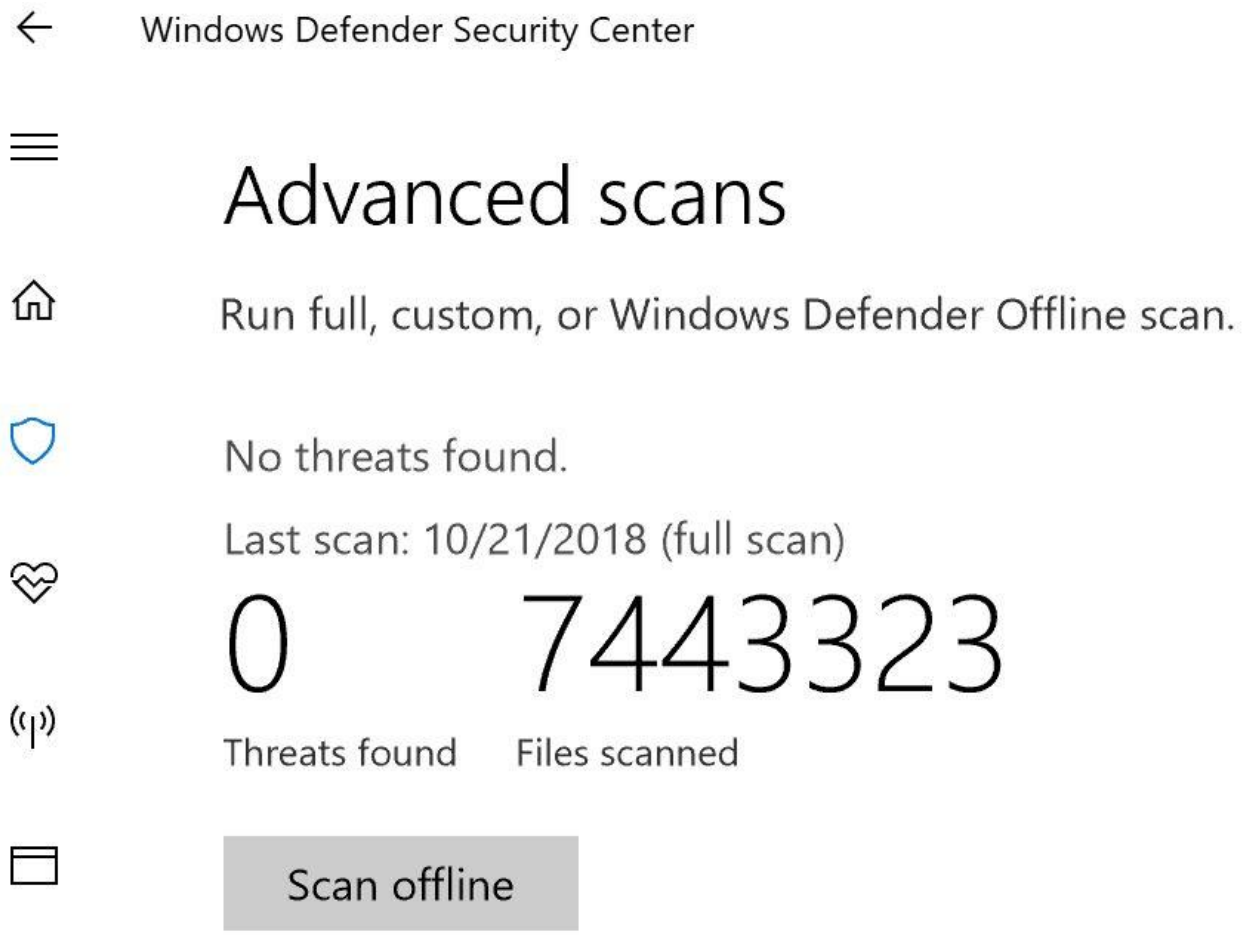
Cyber risk is Operational Risk, but …

…in the world of interconnected computers (a.k.a. "cyberspace"), complexity is extreme and cyber incidents can be highly contagious, so ….

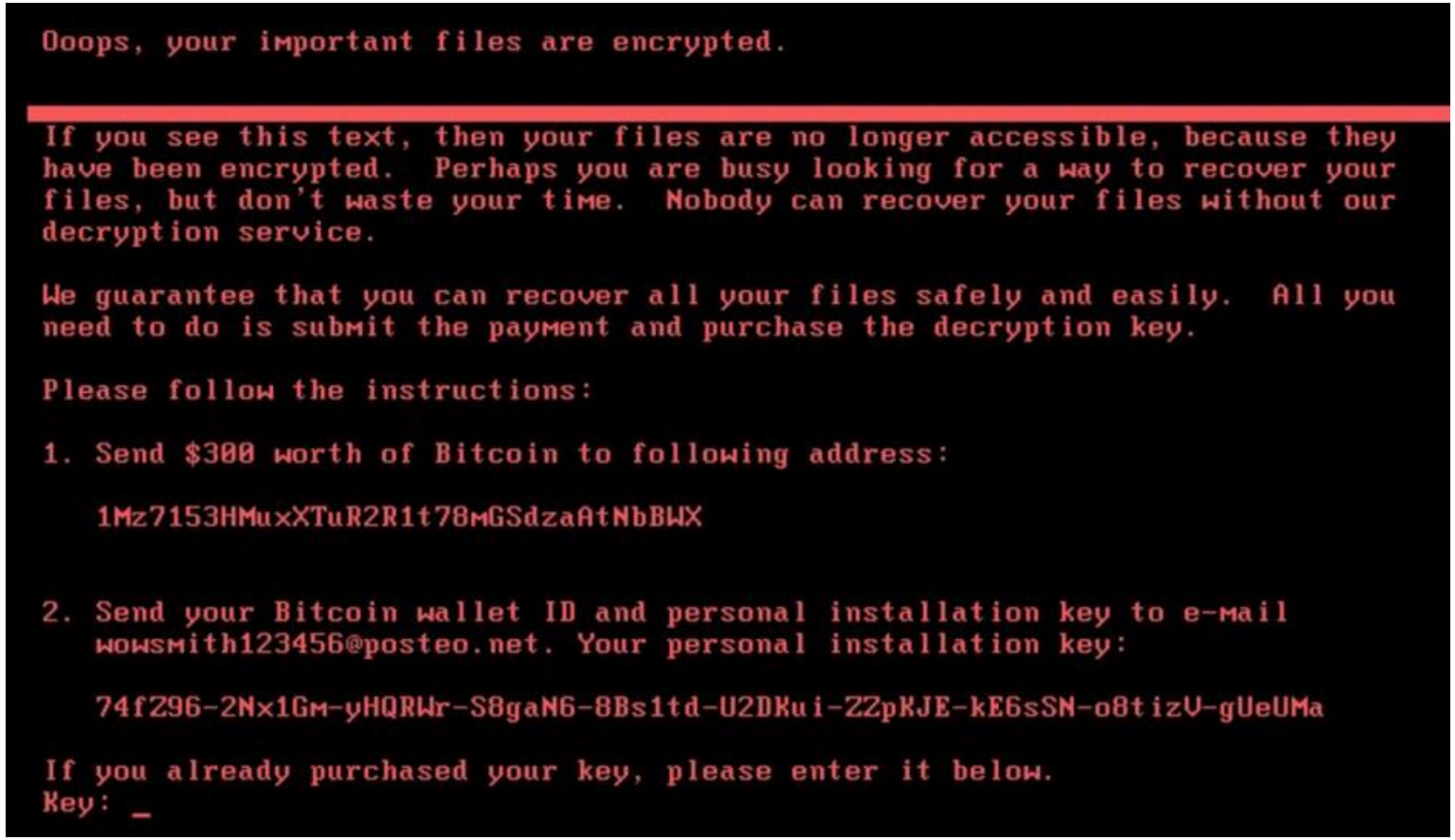
Interconnected Computers??



Complexity???


Windows Defender Security Center
Advanced scans
Run full, custom, or Windows Defender Offline scan.
No threats found.
Last scan: 10/21/2018 (full scan)
0
Threats found
7443323
Files scanned
Scan offline

Contagion???


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-Z2pKJE-kE6sSN-o8tizV-gUeUMa
If you already purchased your key, please enter it below.
Key: _

WORLD BANK GROUP

Cyber risk is Operational Risk, but …

- …the "proportionality" of regulatory requirements and supervisory attention may not apply: all of us may need to be subject to the same "cyber hygiene."

WORLD BANK GROUP

Cyber risk is Operational Risk, but …

…it's no longer clear what role a supervised institution's "risk appetite (or tolerance) for operational risk" (BCP 25) should play in supervisory considerations.

WORLD BANK GROUP

Cyber risk is Operational Risk, but …

… "managing" the risk of outsourcing ICT services to providers such as Amazon, Google, IBM, and Microsoft does not look quite similar to outsourcing cash transportation, or cafeteria and cleaning services! Who is most likely to discover the potential "bugs" and "malware" hidden in the millions of lines of code that make up current software applications?

WORLD BANK GROUP

Who should regulate and supervise cyber risk management in the financial sector?

- As more dimensions of the "production function" of financial services migrate to "cyberspace", authorities other than financial regulators and supervisors will, sooner or later, have a say on what financial institutions must do, or cannot do.

WORLD BANK GROUP

Who should regulate and supervise cyber risk management in the financial sector?

- Financial sector authorities should get actively involved in the process of defining their country's National Cybersecurity Strategy, to better understand with whom they will have to coordinate regulatory and supervisory functions.

WORLD BANK GROUP

Mandatory reporting and incident response

- Financial sector authorities need to know that a cyber incident has taken place in a supervised institution, to estimate its actual or potential impact. Consequently, regulations tend to mandatorily require reporting.
- Technically assisting a supervised institution in handling a cyber incident may, however, not be the financial authorities competitive advantage (vis-à-vis other state agencies) and, if things go wrong, may lead to severe contingent liabilities in some national legal frameworks.

WORLD BANK GROUP

Information sharing

- To share information about cyber incidents, many countries are setting up computer emergency response teams (CERTs), privately or under different State agencies.

- Efficient information sharing requires different "taxonomies" (languages) for different counterparts.

  US Example: Introduction to STIX

WORLD BANK GROUP

What can be done to improve cybersecurity in the financial sector?

Educating Financial Sector Authorities, Board members, Senior Management:

- Cybersecurity is not just a "technical issue," just for the "geeks" working in IT departments and cybersecurity companies! Responding to a cyber incident will frequently require business continuity decisions that cannot be delegated to IT staff.
- FDIC's Cyber Challenge: A Community Bank Cyber Exercise
- World Bank's Cyber-Crisis Simulation Exercises!

WORLD BANK GROUP

What can be done to improve cybersecurity in the financial sector?

Educating the consumer of financial services:

- Computers can do the same things that a phone, a typewriter, or a music player do, but they can also do anything else that somebody programs them to do.
- Because computers are interconnected, somebody can remotely tell our computers to do something we don't want them to do (like revealing the password to our bank account!).
- iPhones and Androids are not "phones", they are permanently interconnected computers with a phone line!

WORLD BANK GROUP
Finance & Markets

Thanks!

aalmansi@worldbank.org