

The Cybersecurity Professional's Current and Future Challenges



1. Why important to businesses
2. Examples
3. How did we got here
4. Concepts and Terms
5. Current & future challenges
6. Summary
7. Questions



ID theft,
Personal security issues
Mitigation measures



Loss to companies:

Intellectual property (IP)

Money/time/distracted 2013 \$3T

Partner and customer trust - Target

Lost jobs - Target, Equifax

Life threatening - Electric grid, Dams, transportation,
and even cars



•
•

- IoTroop may be 1 Million machines worldwide
- Last year Mirai 100,000 machines

- 2.7 M machines, secondary attack 23 machines in 8 countries telcoms
- Concept?
- 4 weeks to discover



- Elmedia (media player)
- Handbrake (video transcoder)
- FOLX (Download manager)
- Information stealing malware





o South Korean web hosting company



- , Tuesday, More than half the victims were in Russia, followed by Ukraine, Bulgaria, Turkey and Japan - ESET
(May) - 200,000
(June)



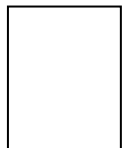




- Massachusetts



China Sinoval & insider employee



Did not even think about security

Speed, cost, functionality, & time to market





poofing,

ampering,

epudiation,

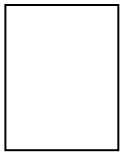
nformation Disclosure,

enial of Service, and

levation of Privilege



○



13 billion years vs. 10 seconds

Kills all encryption schemes

Bad guys- application vulnerabilities

Good guys still learning



Not everyone is vaccinated

Anonymous payment system, Untraceable Source of money

Time, budget, resources,

- o Data - Volume, Velocity, and variety -

- o Hard to analyze, classify, filter and protect



180,000 OSS Projects

1,400 licensing types

More than a million modules

Tested and Secure programming?

18,000 APIs (Expedia, eBay, Salesforce)

Used in many places and companies

Tested and Secure programming?



- 1981

- 32 bit addresses

- 4 billion addresses

~~IBM~~



Still in use since 1960s

Vulnerable

Not patched

Not maintainable

Brittle

No documentation, compilers, hardware



GE 600 offices directly to internet, not corporate network

Saves millions of dollars maintenance, hardware and software

_____ devices connected to networks

Complexity, vulnerabilities, management, ...







