The Cybersecurity Professional's Current and Future Challenges

David C. Brown, PMP, CISSP
CEO/President
Business Complete Solutions
https://www.BusinessCompleteSolutions.com

Agenda

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

Not discussing

- ID theft,
- Personal security issues
- Mitigation measures

Why Important:

Loss to companies:

- Intellectual property (IP)
- Money/time/distraction 2013 $3T
- Partner and customer trust - Target
- Lost jobs - Target, Equifax
- Life threatening - Electric grid, Dams, transportation, and even cars

Examples:

- **Bots and DDOS**
  - IoTroop may be 1 Million machines worldwide
  - Last year Mirai 100,000 machines

- **CCleaner - Software supply chain Attack**
  - 2.7 M machines, secondary attack 23 machines in 8 countries telcoms
  - Concept?
  - 4 weeks to discover

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

- **Ransomware**

NAYANA

  - South Korean web hosting company **Nayana** paid more than $1 million
    - 153 of Nayana's servers
    - 3,400+ websites hosted by the company
    - Many were businesses websites

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

- **IP Theft - Wind Turbine Technology**

- **American Superconductor** - Massachusetts

SINOVEL
华 锐 风 电

- **Wind turbines** China Sinoval & insider employee

BUSINESS COMPLETE SOLUTIONS

How we got here

Did not even think about security

Speed, cost, functionality, & time to market

Terms and concepts

CIA Triad + NA

- Confidentiality
- Integrity
- Availability

+

- Non-repudiation
- Authentication

Attack types: STRIDE

- **S**poofing,
- **T**ampering,
- **R**epudiation,
- **I**nformation Disclosure,
- **D**enial of Service, and
- **E**levation of Privilege

BUSINESS COMPLETE SOLUTIONS

Attacker Steps

1. Reconnaissance,
2. Weaponization,
3. Delivery,
4. Exploitation,
5. Installation,
6. Command & Control (C2), Pivoting,
7. Actions on Objectives
   - Ransomware, exfiltration, disruption, destruction, or Bot

BUSINESS COMPLETE SOLUTIONS

Current and Future Security Challenges

15. Quantum computing

- 13 billion years vs. 10 seconds
- Kills all encryption schemes

14. Machine Learning & AI

- Bad guys- application vulnerabilities
- Good guys still learning
- Can be defeated

13. Changing Attacker profile:

- Nation States - Russia, China, Iran, North Korea- fund, train and protect hackers
- Organized Crime
- Sophistication & Resources
  - It's an industry
- Low Cost and availability of hacking and Ransomware toolkits to millions
- "We are in a cyber war."

12. Expensive security tools

- Not everyone is vaccinated

11. BitCoin

- Anonymous payment system, Untraceable Source of money

10. Complexity -

- Time, budget, resources,
  - Data - Volume, Velocity, and variety -
  - Hard to analyze, classify, filter and protect

9. OSS - Open Source Software

- 180,000 OSS Projects
- 1,400 licensing types
- More than a million modules
- Tested and Secure programming?

8. API - Application Programming Interface

- 18,000 APIs (Expedia, eBay, Salesforce)
- Used in many places and companies
- Tested and Secure programming?

7. IPv4 to IPv6 Migration

- **IPv4**
  - 1981
  - 32 bit addresses

    101.234.012.044
  - 4 billion addresses
- **IPv6**
  - 1998
  - 128 bit address space

    FE80:0000:0000:0000:0202:B3FF:FE1E:8329
  - 34x10^37 addresses

6. Legacy Hardware & Software -

- Still in use since 1960s
- Vulnerable
- Not patched
- Not maintainable
- Brittle
- No documentation, compliers, hardware

5. Threat Intelligence faster, accurate and growing utilization

4. Borderless Networking

- GE 600 offices directly to internet, not corporate network
- Saves millions of dollars maintenance, hardware and software

3. IoT explosion

- **2020 26 Billion** devices connected to networks
- Complexity, vulnerabilities, management, ...

2. New sense of urgency in industry and governments

1. EUBA

- **E**ntity, **U**ser **B**ehavioral **A**nalysis
  - Users, networks and machines

Some Never Learn - Continuing Issues

Ignorance

1. **"I don't need cybersecurity, I have cyber insurance."**
2. **"I am too small for attackers."**
3. **"IT handles our cybersecurity."**

Summary

2021 -

Worldwide Cybercrime damages

- $6 trillion annually

BUSINESS COMPLETE SOLUTIONS

Questions?

David C. Brown, PMP, CISSP
CEO/President
Business Complete Solutions
(412) 357-0266

Dave@BusinessCompleteSolutions.com
https://www.BusinessCompleteSolutions.com