Cybersecurity Career Opportunities

Brett Tucker, PMP, CSBB

March 2019

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0328

Overview

What is Cybersecurity?

Basic Principles

Best Practices

How Can You Make a Difference?

Questions

Who am I?

Education: **Penn State University**

MBA - Business Administration

Old Dominion University

MEM – Engineering Management

University of Notre Dame

BS - Chemical Engineering

Employer: **Carnegie Mellon University** (Pittsburgh, PA)

Software Engineering Institute - CERT Division

Current Position(s): **Technical Manager, Cyber Risk Management**

Adjunct Professor, Heinz College of Information Management, Public Policy, and Management - CMU

Previous Employers(s): Westinghouse Electric Company

Central Intelligence Agency

United States Navy

CARNEGIE MELLON UNIVERSITY

TARTANS

Carnegie Mellon University
Facts and Figures

- Established in 1900
- Global research university of more than 13,500 students
- Carnegie Mellon attracts students from all 50 US states and 93 nations
- CMU Video

- Established as a DoD FFRDC at Carnegie Mellon University in 1984
- Only DoD R&D center focused on software and cybersecurity
- Offices in Pittsburgh, Arlington, and Los Angeles
- About 600 staff (~400 tech staff)

Our Mission and Strategy

To advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

We achieve our mission through

- Research
- Collaboration
- Development and Demonstration
- Transition

In a World of Great Uncertainty

What is Certain?

- Technology will continue to grow in **complexity**
- Organizations must get better at "**surviving**"
- **Knowledge and awareness** must be pervasive throughout the organization
- Traditional tools, techniques, and methods will need to **evolve**
- Organizations must be **agile** enough to adapt

What is Cybersecurity?

What we do…

We attempt to improve computer security

- Think about administrative and physical controls in addition to the technical ones

We study what bad guys do with computers

- Real time observation and forensic

We study why bad guys to what they do.

- So many types of “bad guys” such as states, independent hackers, activists, etc.

Who are the “Bad Guys”?

The rise of the **hacker**

- No longer just hobbyists, now it’s a profession
- State actors with tremendous support
- Criminals still the largest threat—resemble companies with employee benefits
- Anonymous operates in the open, others hide (e.g. Tor)

“Zero-Day Game”

- Race to find vulnerabilities—Symantec says that most flaws go undetected for up to 10 months
- Do “Bug Bounty” programs work?
- Should governments report or exploit them?

Some Basics of Cybersecurity

Who is doing what? What are their motives?

Hackers: Someone who breaks into a computer to Sabotage, Steal, or commit Fraud

Espionage: An individual obtaining information that is considered secret or confidential without the permission

Sabotage: An individual who uses computers to harm an organization or it's data

Fraud: Unauthorized modification, addition, or deletion of an organization's data

How do Hackers Operate?

Phishing: Attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a someone you should trust

Trojan Horse: When a piece of software appears to be one thing but is really something else

Virus: A computer that is infected with unauthorized software, malicious code…it causes the computer to not work properly

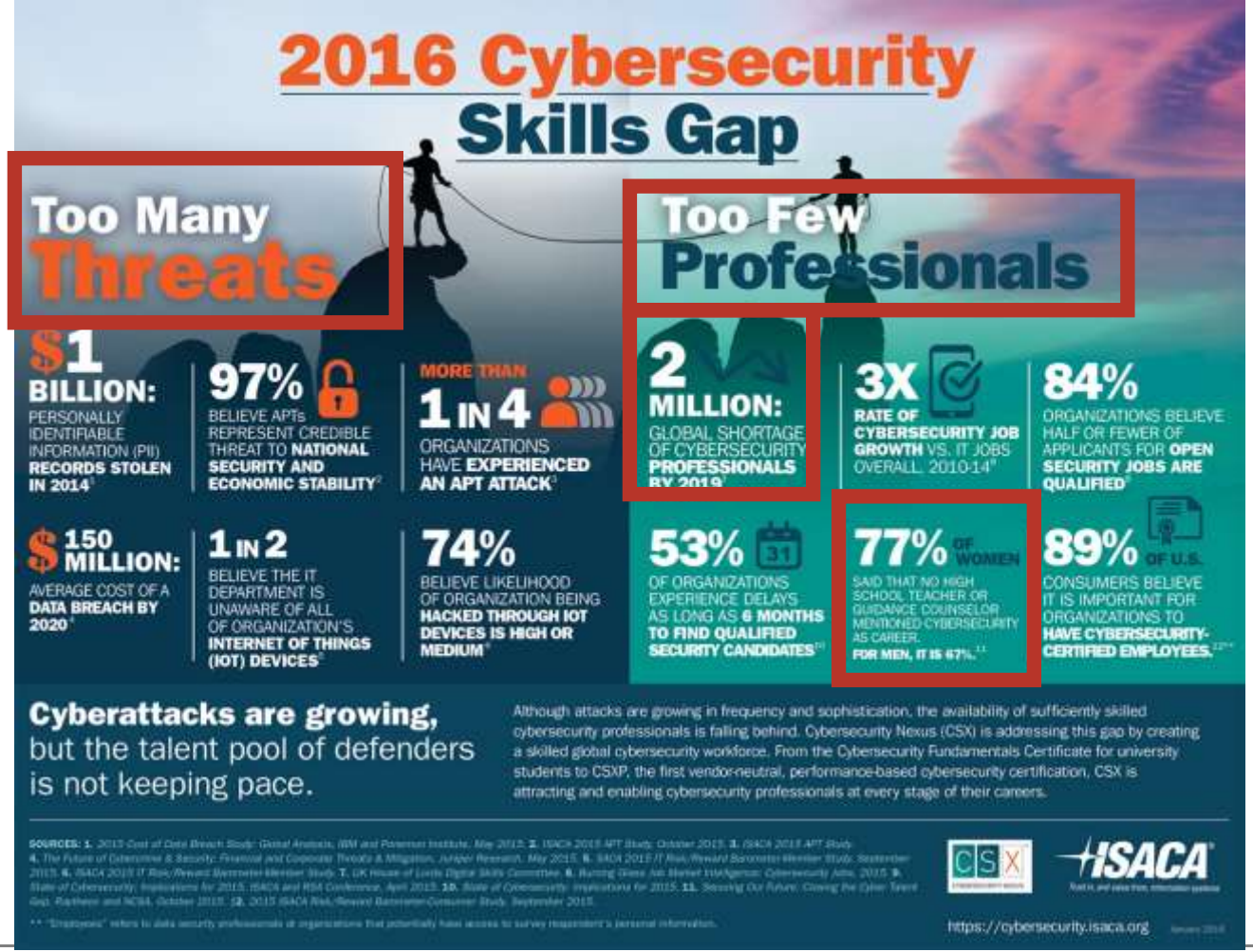
How can you "catch" a virus?

- Download software from internet
- Download music / pictures / song lyrics
- Receive email with an unknown attachment
- Put an unknown CD / DVD into your computer

What Can You Do to Protect Yourself

Basic Cyber Hygiene

- Password protect your computer
- Never go to an untrusted web site
- Never download untrusted software, pictures, songs, or games
- **NEVER** give personal information about your self (name, age, school, address, phone) over the internet
- **Patch, Segment, and Control Administrator Priveleges**



Do You Have What it Takes?

Gorilla Video

Attention to Detail ✓

More than just games…

Learn to navigate the forest…

Build an exciting career…

Decisions are Based Upon Mental Models

Do you naively believe your senses will reveal the world as it is?

Cybersecurity Positions

More Than Just Programming

Focus on

- Math
- Science
- Computing

Other skills that help

- English
  - Be a superlative writer!
- Business classes
- Anything that builds creativity

http://www.cyberdegrees.org/jobs/

Salaries

The Bottom Line

Top Cyber Security Salaries In U.S. Metros Hit $380,000 (January 2016)

Last week we reported that there are over one million cybersecurity job openings in 2016. This week we take a look at the highest paying jobs in cybersecurity.

According to the IT job board DICE, the top IT security salaries go to lead software security engineers who earn an average of $233,333.

SilverBull lists the top six U.S. metros for CISO salaries as follows:

1. San Francisco, Calif. where the average CISO salary is $249,000, and ranges from $154,000 up to $380,000.
2. San Jose, Calif. where the average CISO salary is $240,000, and ranges from $149,000 to $368,000.
3. New York City, N.Y. where the average CISO salary is $240,000, and ranges from $149,000 to $367,000.
4. Washington, D.C. where the average CISO salary is $225,000, and ranges from $139,000 to $334,000.
5. Los Angeles, Calif. where the average CISO salary is $233,000, and ranges from $138,000 to $341,000.
6. Chicago, Ill. where the average CISO salary is $214,000, and ranges from $132,000 to $328,000.

http://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000/#582567f477b4

Salaries

Top U.S. Cybersecurity Salaries Rise To $420,000 (March 2016)

Juniper Research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015.

The cybercrime wave -- along with a severe shortage of cybersecurity workers -- may push CISO salaries closer to the half-million-dollar-per-year mark in the next year or two.

FOR PERSPECTIVE: $420K per year in salary can buy you approximately 1,680 pairs of Air Jordan Tennis Shoes

http://www.forbes.com/sites/stevemorgan/2016/03/15/top-u-s-cybersecurity-salaries-trend-to-420000/#559b975d2f7e

Questions?

Brett A. Tucker, PMP, CSSBB
Technical Manager
Cyber Risk Management
CERT Division
Software Engineering Institute
batucker@CERT.org