Introduction

Let’s talk about security

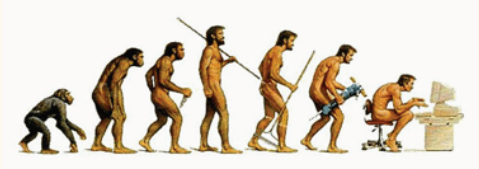
Agenda

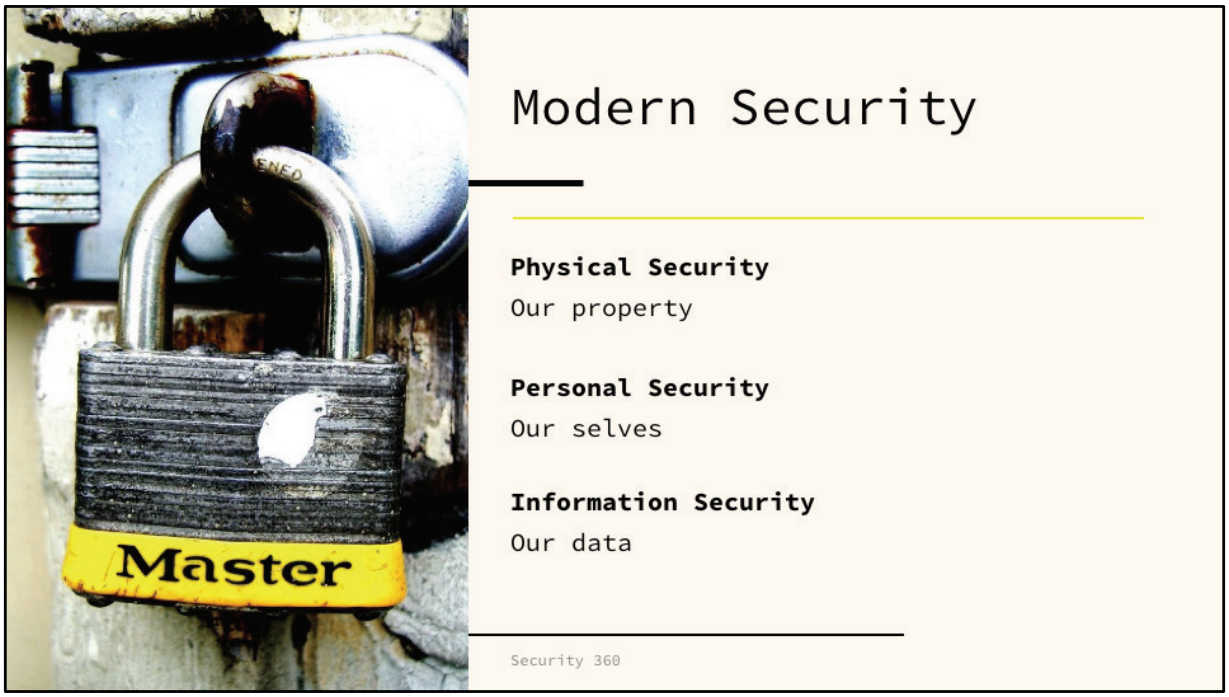
- Security Basics
- Aims & Goals
- A need for Cybersecurity
- Jobs in Cybersecurity

Origins of Security

- *se cura*
  : 'free from' 'care'

- The more things we have,
  the more things we have to secure





Cyber Security

Our electronics

Physical Security
HD / USB / CD

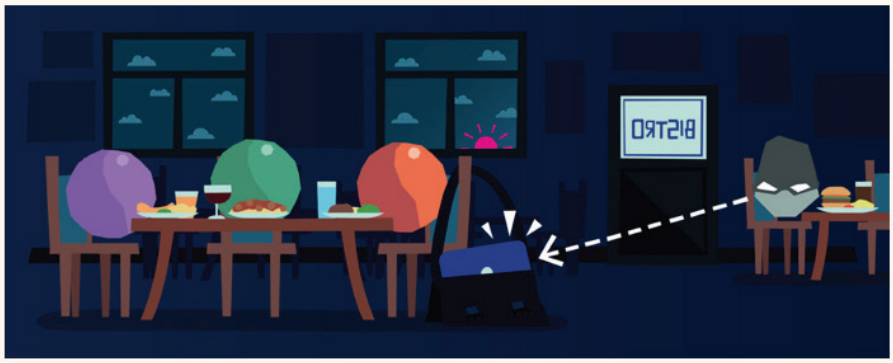
Personal Security
username / password

Network Security
Computer / Mobile / IoT

Security 360

Physical Security

- A.K.A Physical Security



Security 360

Personal Security

- A.K.A. Social Engineering

Security 360

Network Security

- A.K.A. Internet Security

Security 360

Cyber Security

Our electronics

Personal Security
username / password

Physical Security
HD / USB / CD

Network Security
Computer / Mobile / IoT

Security 360

Cyber Security

Our electronics

Perso l S uri

u rd

Information Security

Data

ty

Computer / Mobile / IoT

Security 360

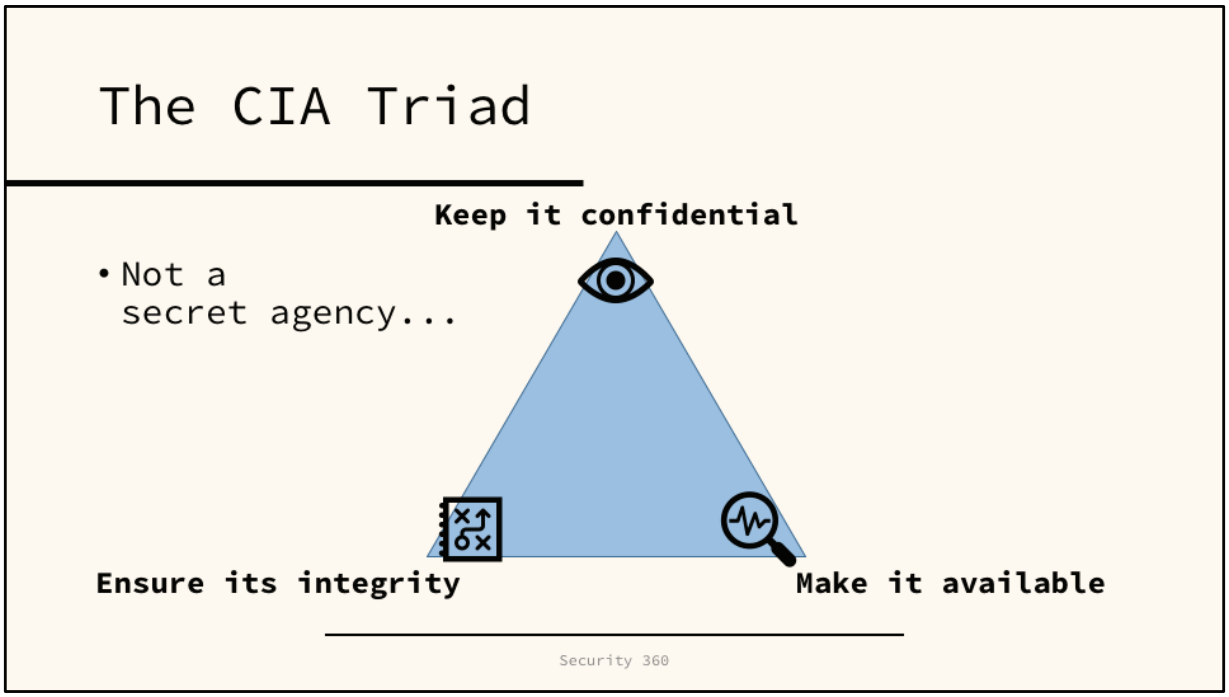
Information Security noun

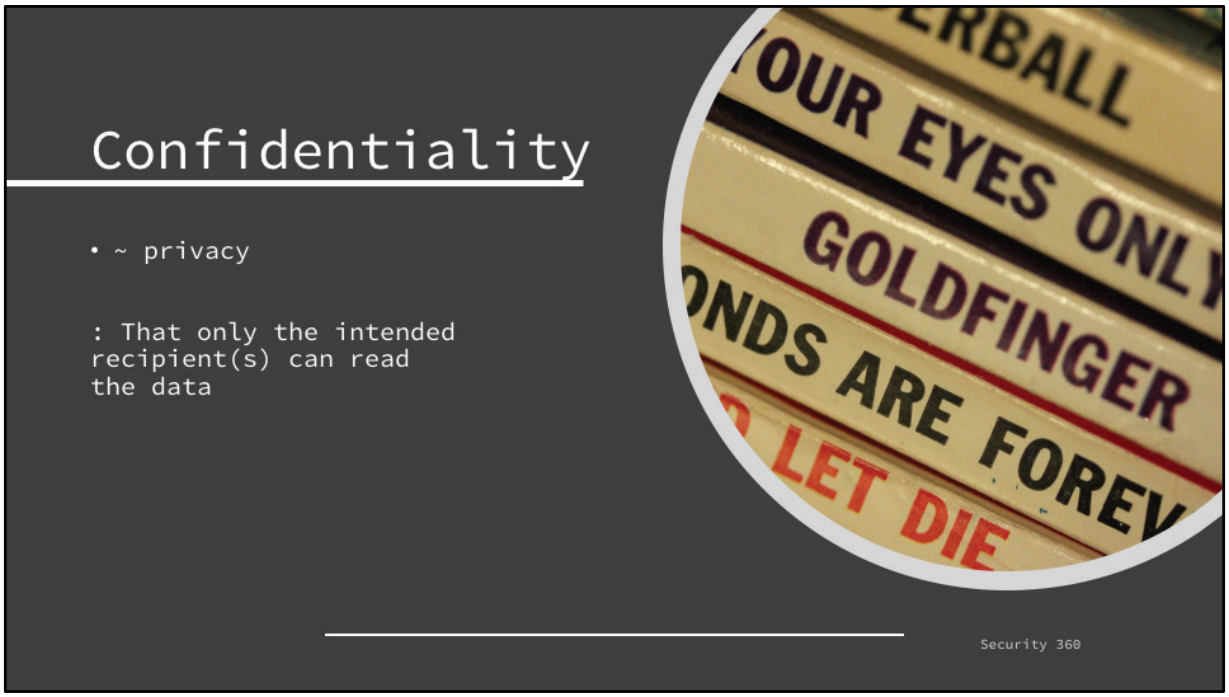
: The protection of information and information systems from
unauthorized access, use, disclosure, disruption, modification, or destruction

in order to provide
confidentiality, integrity, and availability

44 U.S. Code § 3542

Security 360





Availability

- 24/7/365

: That the data can be accessed at *any* time

Security 360

Information Assurance noun
AKA Cybersecurity noun

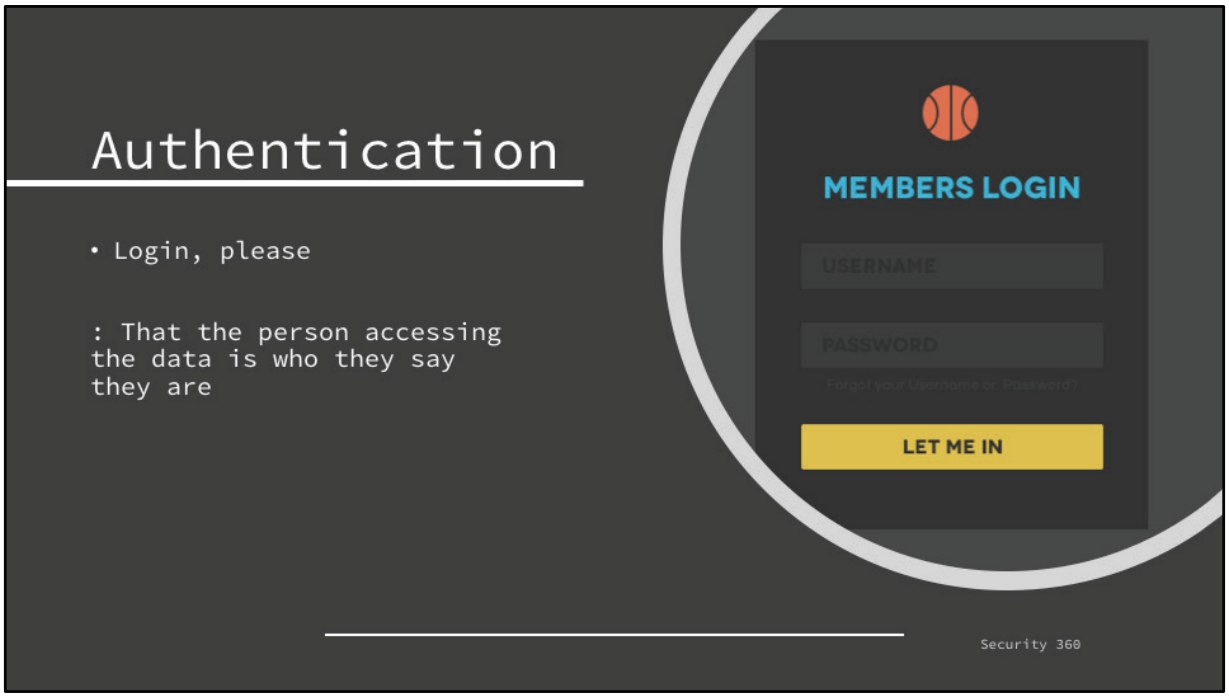
Measures that **protect** and **defend** information and information systems

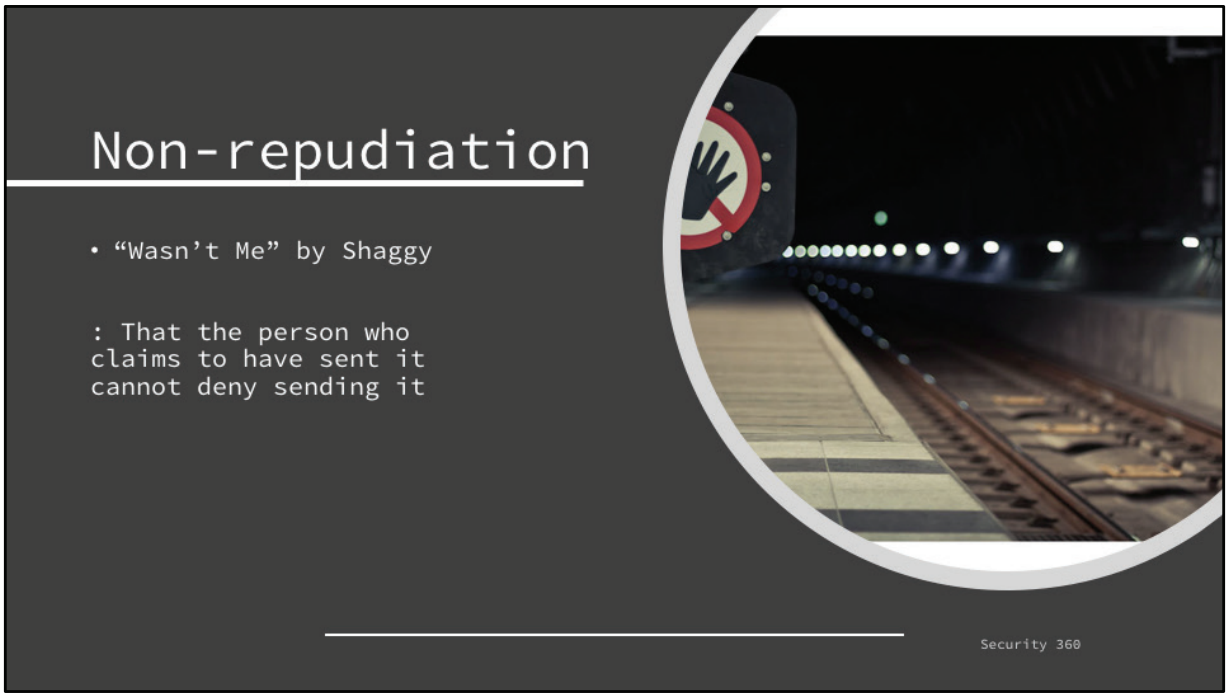
by ensuring their

availability, integrity, **authentication**, confidentiality, and **non-repudiation**

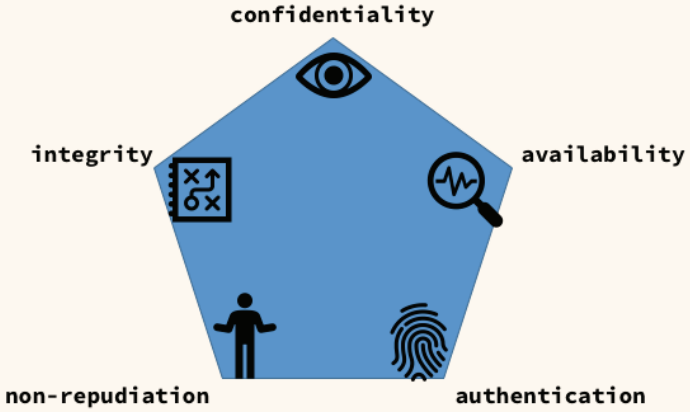
CNSSI-4009

Security 360





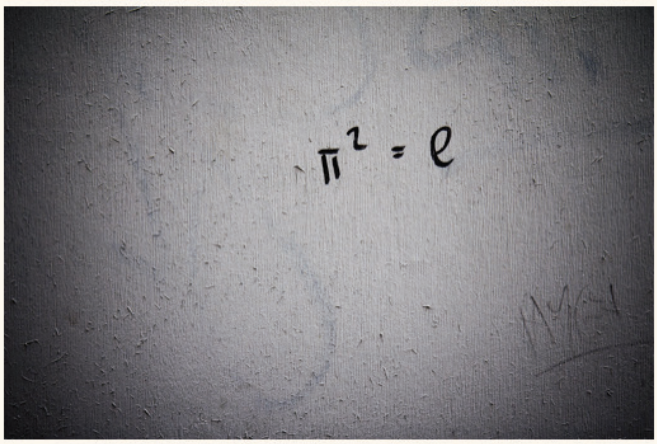
The CIAAN Pentagon



Security 360

Solving the Pentagon

- Confidential
  - Encrypt it
- Integrity
  - Compare Copies
- Availability
  - Build it well
- Non-repudiation
  - Sign it
- Authentication
  - Passwords/Fingers



Solving the Pentagon

- In fact, **most** of the goals of cyber security can be solved with the help of one science

CRYPTOLOGY!
: The science of securing communication

(but let's save that for tomorrow)

Most?

- Cryptology can’t solve everything
- The obvious one:
  - Availability
- The not-so obvious one:
  - Authentication (though cryptography is most of it)

Availability

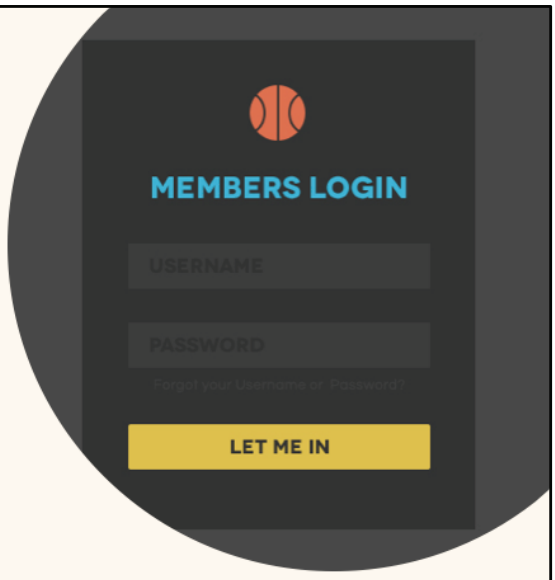
- That the data can be accessed at *any* time

- Well-built
  - Reliable hardware
- Well-maintained
  - Regular updates
- Well-secured
  - Best practices

Security 360

Authentication

- ...please enter your password
- If your password can be guessed, no amount of cryptographic encryption can save you



Password Faux-Pas

- If you use the word “password” in your password, you’ve got a problem
- If you use your birthdate in your password, you’ve got a problem
- If you can find your password in a dictionary, you’ve got a problem

https://howsecureismypassword.net/

Have I Been Pwned?

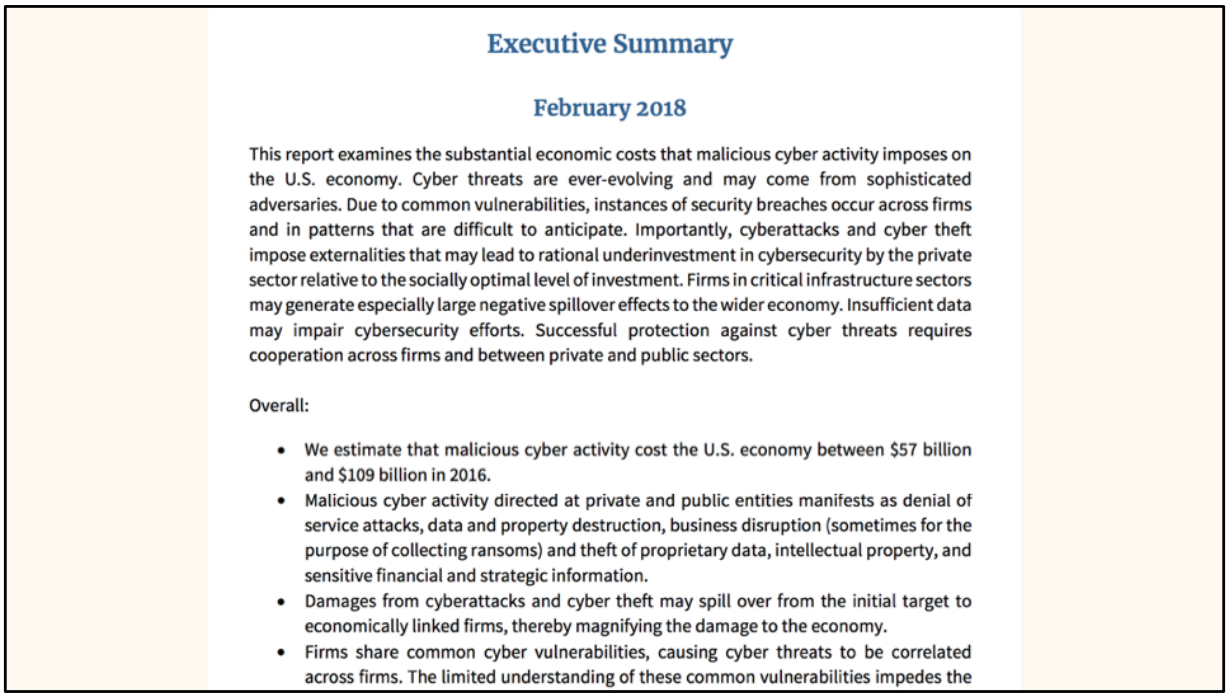
https://howsecureismypassword.net/

Password Must-Dos

The current recommendation:

- Think of a memorable phrase
  - I like to study cyber security with Jay in Paris
- Put a number and symbol in somewhere
  - I like 2 study cyber security with Jay in Paris!
- Take the first letter of each word/symbol
  - **I** **l**ike **2** **s**tudy **c**yber **s**ecurity **w**ith **J**ay **i**n **P**aris**!**
- Voila! Secure password
  - Il2scswJiP!

Why should we care?



Executive Summary

February 2018

This report examines the substantial economic costs that malicious cyber activity imposes on the U.S. economy. Cyber threats are ever-evolving and may come from sophisticated adversaries. Due to common vulnerabilities, instances of security breaches occur across firms and in patterns that are difficult to anticipate. Importantly, cyberattacks and cyber theft impose externalities that may lead to rational underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment. Firms in critical infrastructure sectors may generate especially large negative spillover effects to the wider economy. Insufficient data may impair cybersecurity efforts. Successful protection against cyber threats requires cooperation across firms and between private and public sectors.

Overall:

- We estimate that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.
- Malicious cyber activity directed at private and public entities manifests as denial of service attacks, data and property destruction, business disruption (sometimes for the purpose of collecting ransoms) and theft of proprietary data, intellectual property, and sensitive financial and strategic information.
- Damages from cyberattacks and cyber theft may spill over from the initial target to economically linked firms, thereby magnifying the damage to the economy.
- Firms share common cyber vulnerabilities, causing cyber threats to be correlated across firms. The limited understanding of these common vulnerabilities impedes the

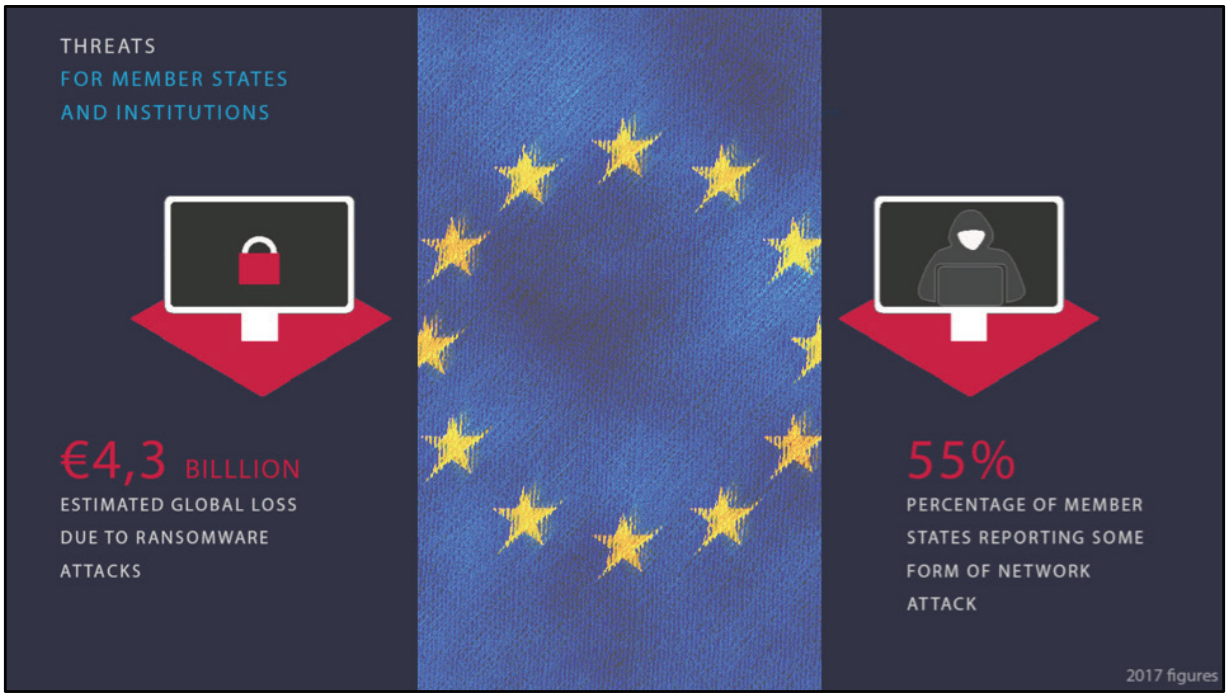
https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Table 2: Table of Security Incidents and Breaches by Sector, 2016

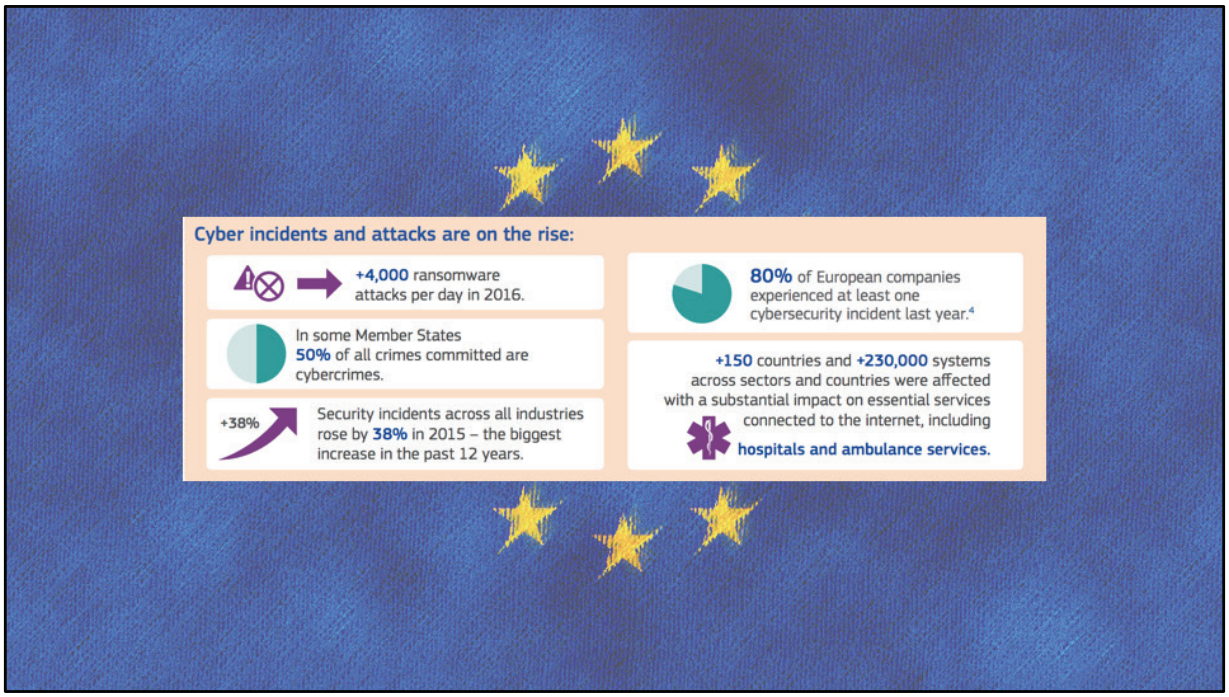
	Incidents				Breaches			
	Total	Small	Large	Unknown	Total	Small	Large	Unknown
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51

Note: Left columns indicate all security incidents, while the right columns indicate breaches.
Source: Verizon (2017).

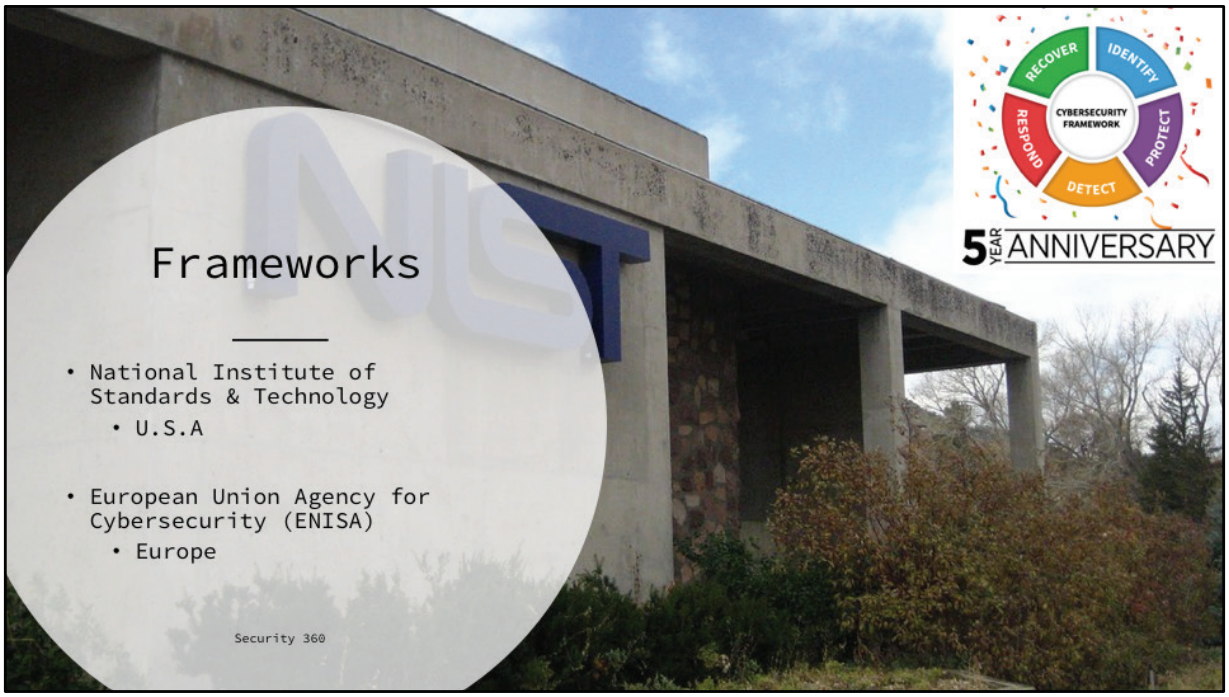
https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf



https://www.consilium.europa.eu/en/infographics/cyber-security/
"EU flag" by *BalkanPhotos* is licensed under *CC CC0 1.0*



https://www.consilium.europa.eu/en/policies/cyber-security/cybersecurityfactsheet.pdf



Standards

- International Organisation for Standardisation
- ISO27000 family of standards
  - 27001: Infosec Management
  - 27002: Code of Practice
  - 27003: Implementation
  - 27004: Metrics
  - 27005: Risk Management
  - 27006: Certification
  - 27007: Audits

Jobs in Cybersecurity

Network Engineer

Learn the basics

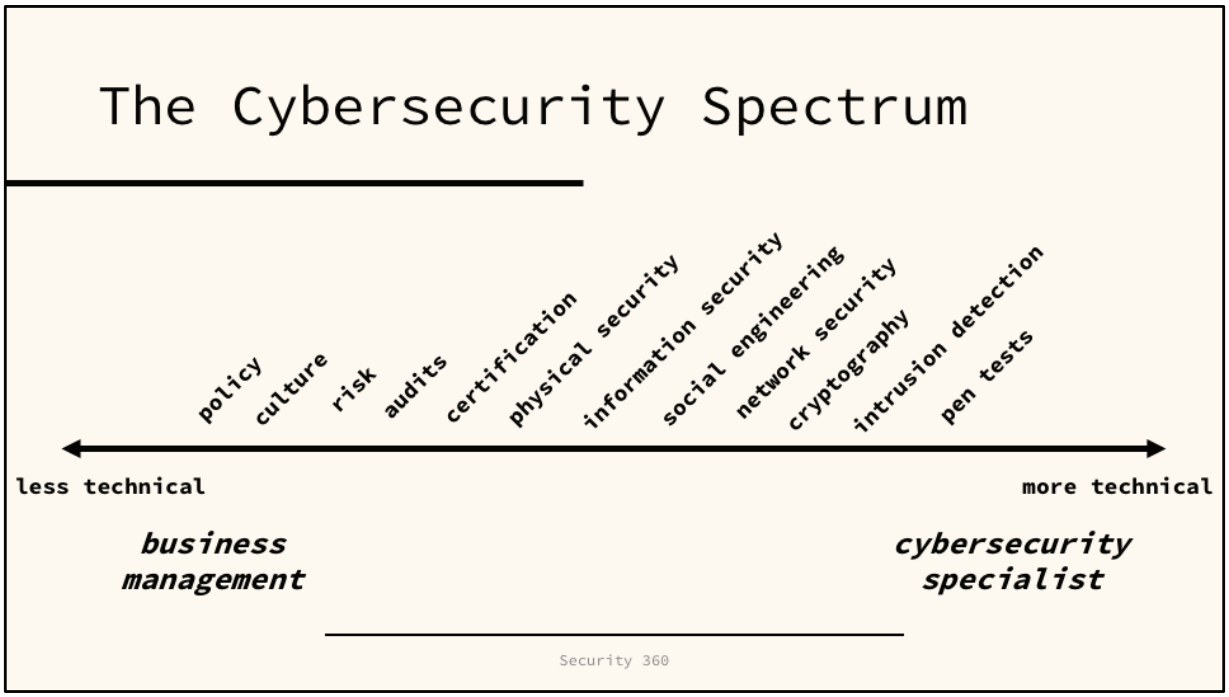
Cybersecurity Specialist

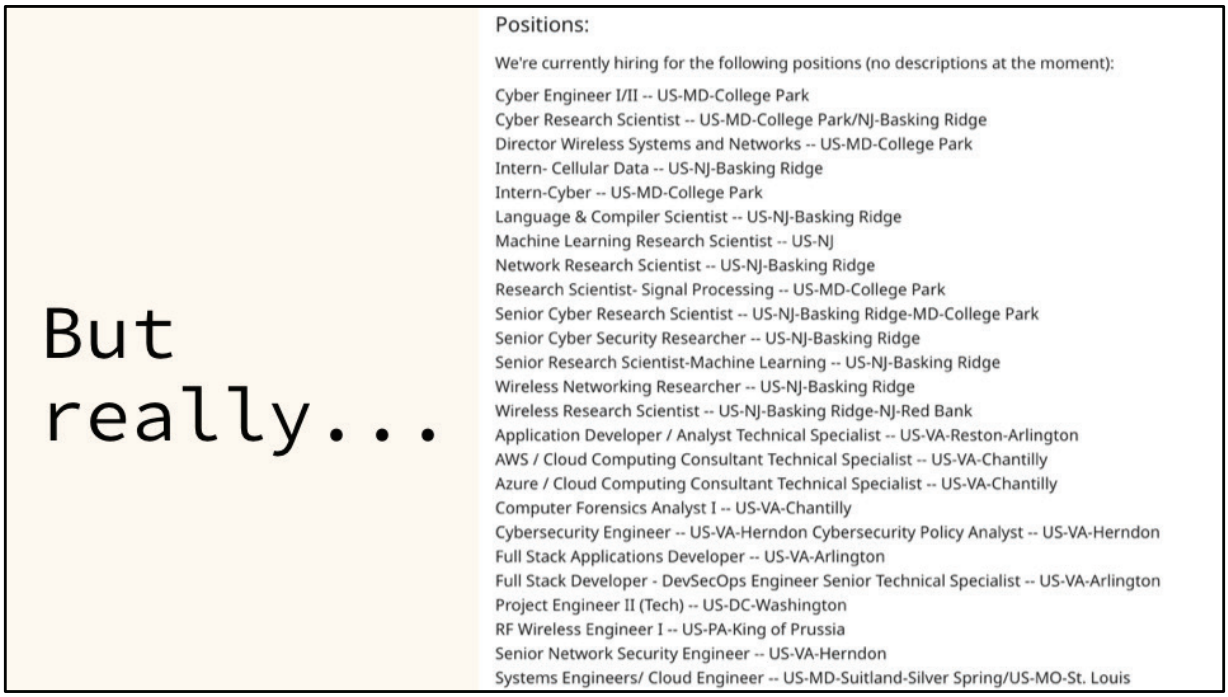
Apply knowledge on a red team / blue team

Security Management

Make policy & define culture

Security 360


The Cybersecurity Spectrum
policy
culture
risk
audits
certification
physical security
information security
social engineering
network security
cryptography
intrusion detection
pen tests
less technical
more technical
business management
cybersecurity specialist
Security 360



Secure Consulting Solutions, LLC

Company Overview:
Secure Consulting Solutions, LLC (SCS), is an Information Technology (IT) Cyber Security services firm with a core focus on Innovative Cyber Security Solutions in Web Application and Mobile Application Security. SCS, founded in 2014 and headquartered in Washington, DC, was established to help commercial and government entities meet the complex and growing technical cyber security challenges faced on a daily basis and strategically plan for the cyber challenges that will be faced in the future.

Certification

- Degrees
  - Short programs
  - BSc Cybersecurity
  - MSc Cybersecurity
- Industry Certs
  - Security+
  - CISSP
  - OSCP
  - GIAC/SANS

Security 360

Job Hunting

https://www.cyberseek.org/heatmap.html

Consulting

- In the traditional sense
  - Contracted
  - Offer advice to a company
  - Company implements the advice independently
- For some specialised roles (i.e cybersecurity)
  - Still contracted
  - Still offering advice
  - Also working on implementation
    - Sometimes as the only engineer!

Security 360

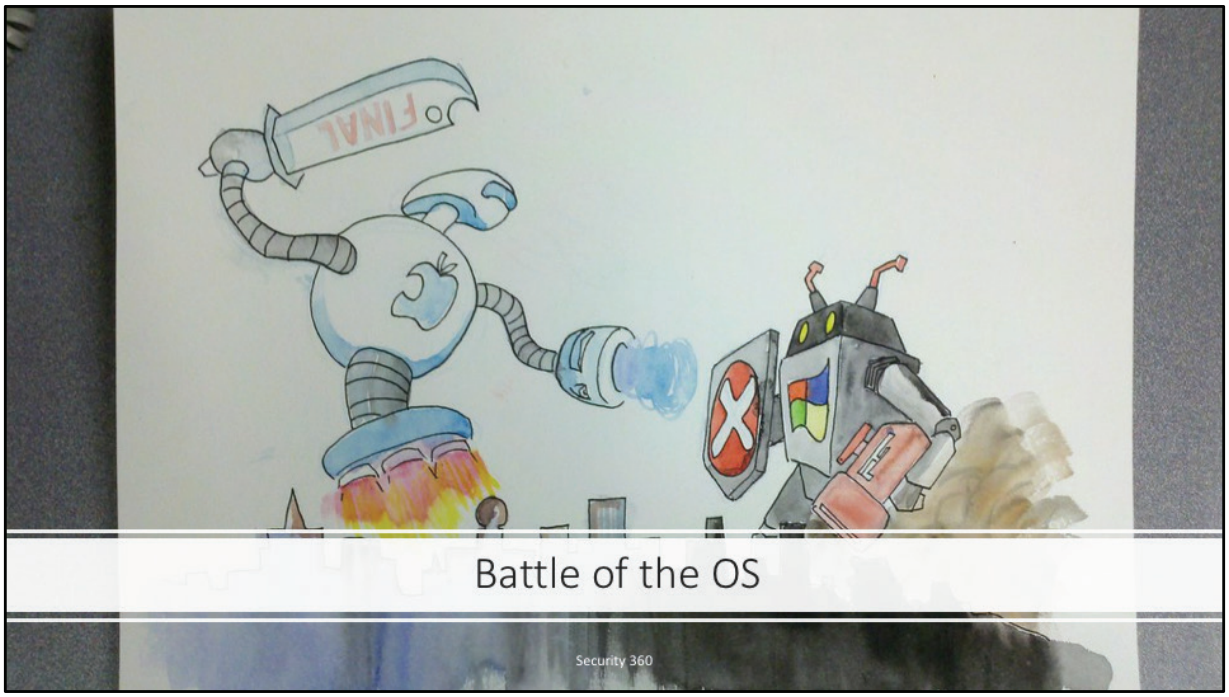
Consultancy vs Permanency

Many different workspaces	More job stability
Many different people	More benefits
Wider range of skills	More regular hours
Higher hourly pay	More familiarity
Higher pay ceiling	See projects through
	Easier to start

Security 360

Where to start??


root@jaysmac # banner -w 34 Linux
root@jaysmac #



About Linux

- Unix-like
  - Mac OS
  - Android
  - Chrome OS
  - But **NOT** Windows
- 1991, started by a Computer Science student
  - Linus Torvalds
- Open-Source (FREE)
  - https://github.com/torvalds/linux

GNU (GNU's Not Unix)

- An OS started in 1983
- Mostly finished in 1991, except for the Kernel
  - GNU/Linux!
- Adds basic, higher-level function to the Kernel
  - Copy, write, remove, edit

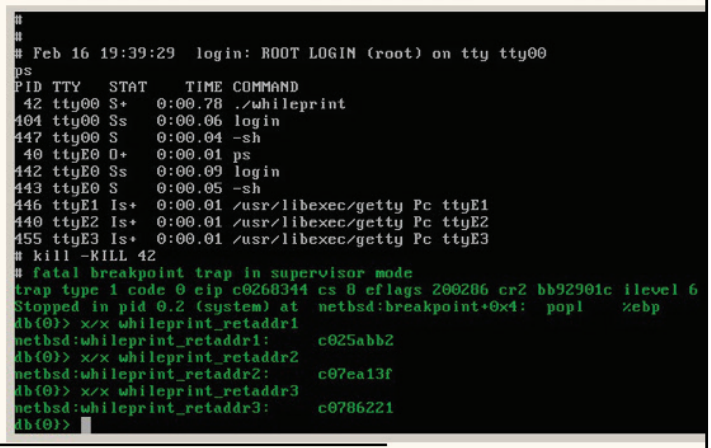
Linux Distros

Extend GNU/Linux: UX, GUI, more tools, more fun

- Debian GNU/Linux
  - Very early, 1993
- Ubuntu by Canonical
  - Based on Debian, came much later (2004)
- Fedora/RHEL/CoreOS

Security Distros

- Knoppix
  - Run from USB
  - Mostly forensics
- BackTrack
  - Add more sec tools
- Kali Linux
  - Based on Debian
  - By the OSCP team!



Security 360

Where is it?

- Supercomputers
- Data Centres
- Servers

- Your neighbourhood hacker's laptop

https://linuxjourney.com