Introduction to the Class, 2021-01-19

Sony Pictures 2014 breach:

- http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html
- https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack

Course objective 1

Explain cybersecurity as a key enterprise risk and how it can be managed.

Even small businesses need to achieve three security objectives:

- Confidentiality: The impacts of a breach of confidentiality of financial management information are generally associated with the sensitivity of the existence of projects, programs, and/or technologies; and customers, suppliers, contractors and employees that might be revealed by unauthorized disclosure of information.
- Integrity: The impacts of a breach of integrity of financial management information may result from temporary successful frauds that can affect the business' image, while corrective actions may disrupt the business' operations.
- Availability: The impacts of a permanent loss of availability of financial management information can cripple business operations.

Security is not the same as safety:

> "Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time."
>
> Bruce Schneier, *Security Engineering*, p. xxvii.

Types of attackers:
1. Rogue hackers
2. Organized crime
3. Insiders
4. Nation-states

Rogue hackers:

- Twitter hack of 2020:
  - https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html
- Capitol One Breach by a single individual: https://www.nytimes.com/2019/08/14/technology/capital-one-hacking.html
- Hacktivist attack on nearly 1,000 politicians and journalists:
  - https://www.nytimes.com/2019/01/04/world/europe/germany-hacking-politicians-leak.html?module=inline
  - https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html
- Breach of Hacking Team:
  - http://arstechnica.com/security/2016/04/how-hacking-team-got-hacked-phineas-phisher/

Organized crime:

- Credit card theft today: https://krebsonsecurity.com/2017/12/4-years-after-target-the-little-guy-is-the-target/
- Sale of credit cards from HyVee breach: https://krebsonsecurity.com/2019/08/breach-at-hy-vee-supermarket-chain-tied-to-sale-of-5m-stolen-credit-debit-cards/
- Zeus malware and Evgeniy Mikhaylovich Bogachev:
  - FBI Most Wanted, $3 million bounty: https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev/@@download.pdf
  - "Russian Espionage Piggybacks on a Cybercriminal's Hacking," https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html
  - "Chasing the Phantom: Inside the Hunt for Russia's Most Notorious Hacker," https://www.wired.com/2017/03/russian-hacker-spy-botnet/
- 2016 Bangladesh central bank hack of $101 million dollars
  - Attempted theft of $1 billion thwarted in part due to a typo
  - The U.S. indicted Park Jin Hyok, an individual associated with the North Korean government, with involvement in the attack: https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html
  - Video report: https://youtu.be/6Y9UaLKbZQ0
  - Lawsuit filed by Bangladesh bank: https://www.wsj.com/articles/bangladesh-bank-sues-filipino-lender-in-u-s-court-over-hack-heist-11549294562

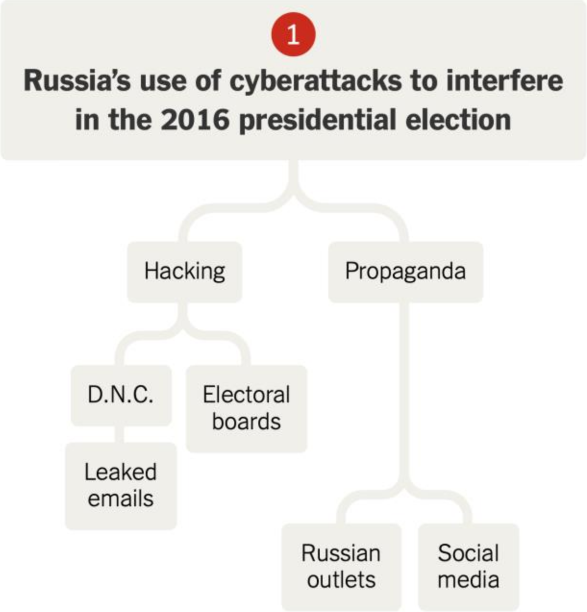
Insiders:

- Edward Snowden:
  - https://en.wikipedia.org/wiki/Edward_Snowden
  - Deliberately chose to work for Booz Allen Hamilton to gain access to the NSA: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/10140223/Edward-Snowden-admits-infiltrating-contractor-to-harvest-documents.html
- Harold T. Martin:
  - https://www.nytimes.com/2018/01/03/us/politics/harold-martin-nsa-guilty-plea-offer.html
  - "The NSA Officially Has a Rogue Contractor Problem," https://www.wired.com/story/nsa-contractors-hacking-tools/
  - Kaspersky Labs tipped off NSA to Martin: https://www.politico.com/story/2019/01/09/russia-kaspersky-lab-nsa-cybersecurity-1089131

Nation-states

- China, advanced persistent threat (APT):
  - December 21, 2018: APT 10 Indictment (includes video): https://www.washingtonpost.com/world/national-security/us-and-more-than-a-dozen-allies-to-condemn-china-for-economic-espionage/2018/12/20/cdfd0338-0455-11e9-b5df-5d3874f1ac36_story.html
  - "Chinese Businessman Sentenced to Prison for Hacking U.S. Contractors," https://www.nytimes.com/2016/07/14/us/chinese-businessman-hacking-prison.html
  - "Man Who Sold F-35 Secrets to China Pleads Guilty," https://news.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty
  - Lockheed Martin F-35 and Chinese J-20 compared: https://www.businessinsider.com/americas-f-35-fighter-jet-vs-chinas-j-20-2016-12

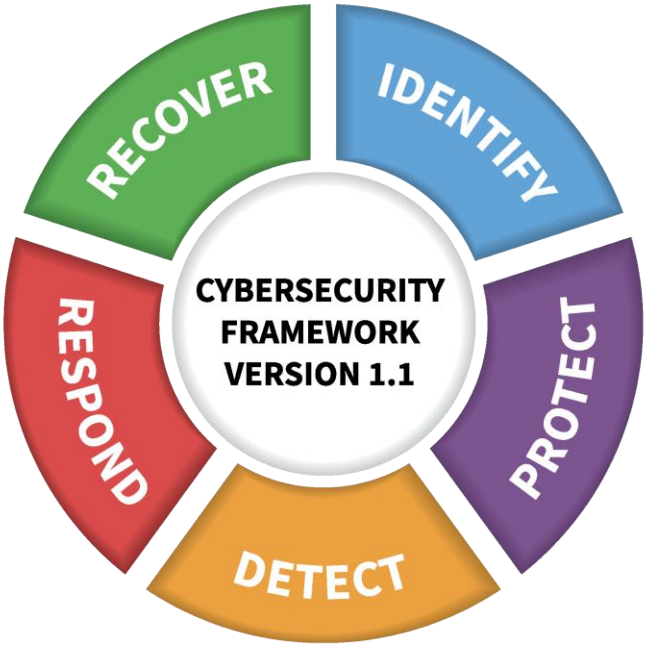
    - RSA breach: https://www.wired.com/2011/08/how-rsa-got-hacked/
    - Marriott breach:
        - https://www.nytimes.com/2019/01/04/us/politics/marriott-hack-passports.html
- Election influence campaigns:
    - Macron doxing: https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html
    - Department of Justice indictment of 12 Russian operatives for interfering with US elections: https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html
    - Summary of Russia's interfering efforts: https://www.nytimes.com/interactive/2017/12/10/us/politics/trump-and-russia.html



- North Korea:
    - It's Official: North Korea is Behind WannaCry: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537
    - North Korea agent indicted for Sony hack, Bangledesh Bank theft of $101 million dollars: https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html
    - "Philippine court orders jail for former bank manager over Bangladesh central bank heist," https://www.reuters.com/article/us-cyber-heist-philippines/philippine-court-orders-jail-for-former-bank-manager-over-bangladesh-central-bank-heist-idUSKCN1P40AG
    - Sony hack inside stories:
        - https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg
        - http://fortune.com/sony-hack-part-1/
- Cyberwar:
    - Overview: https://www.youtube.com/watch?v=mtBnu-YtibA
    - Stuxnet: https://en.wikipedia.org/wiki/Stuxnet

NIST Cybersecurity Framework:

- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf



Course objective 2

Apply methods to identify, protect against, detect, respond to, and recover from cybersecurity threats.

Course objective 3

Use techniques of ethical hacking to perform penetration testing.

Course objective 4

Communicate risk assessment reports that support management decisions.