ACS-2821-001

Information Security in Business

# Securing the Future

# ACS-2821-001 – Slides Used In The Course

THE UNIVERSITY OF WINNIPEG

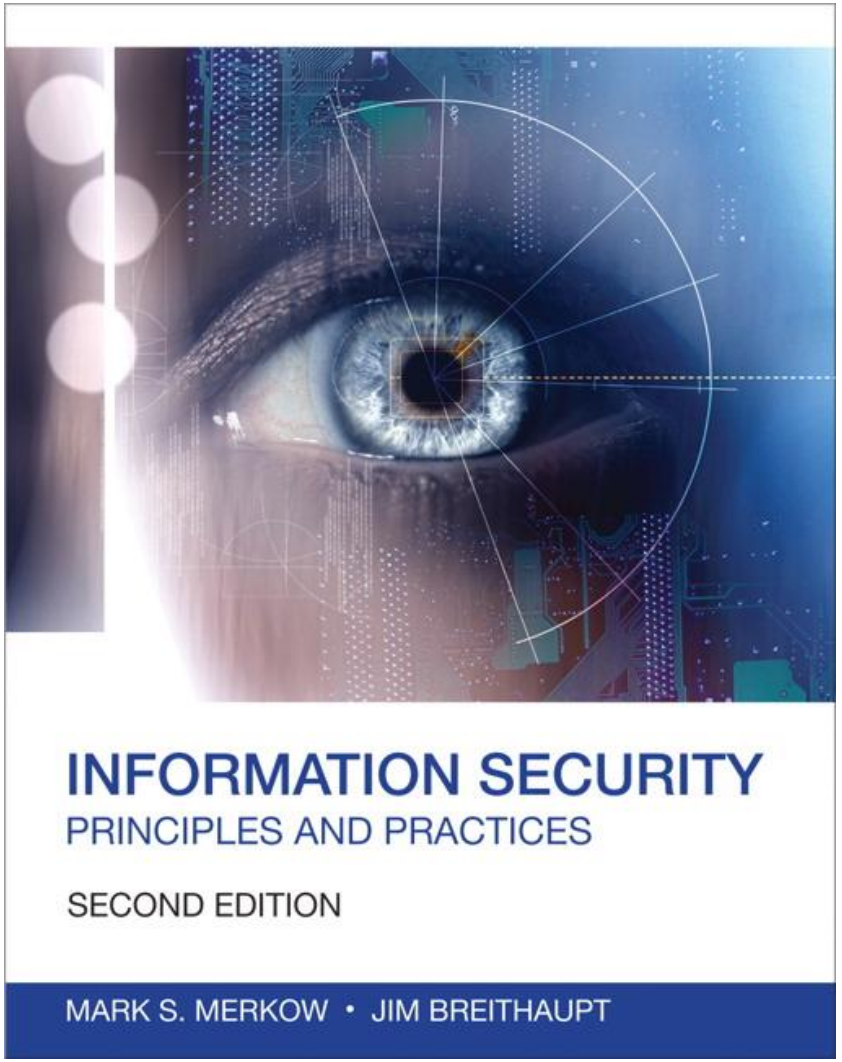
## A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.





# Objectives

- Follow the evolution of increased cybercrime and efforts to reduce cybercrime
- Discuss the future of information technology (IT) software security developments and the outlook for InfoSec professionals
- Discuss the trends that drive the growth of the industry, technology, and regulations

# Operation Eligible Receiver

- In1997, Operation Eligible Receiver demonstrated a potential vulnerability of U.S. government IT systems
  - 35 hackers were hired by NSA to launch a simulated attack
  - They obtained administrative access in 36 out of 40,000 systems
- The exercise set the stage for a widespread national initiative called Critical Infrastructure Protection (CIP)
  - In 1998, President Clinton signed Presidential Decision Directive (PDD) Number 63 to establish the program

# Operation Eligible Receiver

- Most of the government activity that began from PDD63 has continued and is now led by the Department of Homeland Security
- Information Sharing and Analysis Centers (ISACs) have been expanded from the original 8 sectors to 15, with varying degrees of participation
  - An example is the Financial Services ISAC (FS/ISAC) for the banking and finance sector

# Carders, Account Takeover, and Identity Theft



- Carder sites
  - A web site where stolen information such as credit card numbers, PINs, and Social Security numbers are traded
- Credit card fraud
  - When stolen credit card data is used for transactions
- Account takeover
  - When stolen log-in credentials access a private bank or credit card account
- Identity theft
  - When stolen personally identifiable information (PII) is used to open new lines of credit unknown to the victim

# ZeuS Banking Trojan

- First detected July 2007
- Written for Windows and used to attack the U.S. department of Transportation
- Steals data from infected computers through a web browser and protected storage
  - The infected computer sends the stolen data to a bot command and control server
  - Sold in the criminal underworld as a kit

# Phishing and Spear Phishing



- Phishing attacks are on the rise, and user computers are being infected by Keystroke loggers and Trojan horses allowing the attacker to own the computer and steal sensitive information
- Spear phishing
  - Directed to specific targets

# Other Trends in Internet (In)Security



- Stuxnet worm
  - Discovered in 2010 and used to take control over Iranian nuclear enrichment facilities
  - Ultimate goal was to access SIMATIC WinCC SCADA used as industrial control systems in pipelines, power plants, airports, ships, and other important infrastructures

# Other Trends in Internet (In)Security



- Blockchain and cryptocurrency
  - Stuart Haber and W. Scott Stornetta in 1991 first describe what a blockchain is
  - First blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008 and in 2009 bitcoin was created
  - Blockchain has an environmental cost
    - Blockchain relies on encryption to provide its security
    - complex algorithms must be run, and large amounts of computing power

# Other Trends in Internet (In)Security

THE UNIVERSITY OF WINNIPEG

- Blockchain and cryptocurrency
  - Lack of regulation creates a risky environment
    - Lack of regulatory oversight, scams and market manipulation are commonplace
    - Example - Oncecoin was revealed as a Ponzi scheme robbing millions from investors
    - there is always a chance that the exchange or online wallet where you keep your coins will be hacked, shut down by governments due to shady practices, or simply abscond with your coins
  - Its complexity means end users find it hard to appreciate the benefits
  - Blockchains can be slow and cumbersome
  - The “Establishment” has a vested interest in blockchain failing

# Other Trends in Internet (In)Security

THE UNIVERSITY OF WINNIPEG

- Artificial Intelligent and Machine Learning
  - The field of AI started back in 1956 at Dartmouth College
  - AI revolved around the use of algorithms
  - Since AI use algorithms, how can we guard against mistakes?
  - Human design these algorithms for AI, so how do we eliminate AI bias
  - Security, how do we keep AI safe from adversaries and other AI adversaries
  - And the threat of “The Terminator” or the “Cylone” from Battlestar Galactica – Hollywood depiction of future AI
  - Rise of the robot with intelligent.

# Other Trends in Internet (In)Security



- Quantum computing and Quantum cryptography
  - In 1959, Richard Feynman, in his lecture "There's Plenty of Room at the Bottom“ describe the possibility of using quantum effects for computation
  - January 2019, IBM launched IBM Q System One, the first integrated quantum computing system for commercial use.
  - A quantum computer could efficiently solve integer factorization, which underpins the security of public key cryptographic systems using the Shor's algorithm
  - Quantum cryptography could potentially fulfill some of the functions of public key cryptography
  - Also some public-key algorithms that are not based on integer factorization and discrete logarithm problems are not affected
  - NIST has put out RFC on quantum-based cryptographic systems

# The Rosy Future for InfoSec Specialists

THE UNIVERSITY OF WINNIPEG

- Demand for information security expert is outstripping the available supply by a widening margin
- In addition, information security professionals may find themselves in positions of higher responsibility in coming years

# Summary

- Constant vigilance and monitoring are critical to keeping systems safe and secure
- Security experts must improve their ability to predict and not just react to the future
- Creating a culture of information security specialists is critical to advances in information security

# ACS-2821-001 – Questions?