CIS377-407
Introduction to Cybersecurity

Dr. Atul Rawal

Instructor Information

Atul Rawal, Ph.D.

- Experience -
  - Sr. Data Scientist - xD | U.S. Census Bureau.
  - Postdoctoral Research Fellow - U.S Food & Drug Administration.
  - Visiting Research Fellow - U.S Army DEVCOM Army Research Lab.
  - Ph.D. Student & Research Associate - U.S DoD Center of Excellence in AI/ML (CoE-AI/ML) Howard University.
  - Ph.D Student & Adjunct Faculty – Towson Univ.
- Education –
  - B.Sc. in Physics (High Energy Physics)
  - Ph.D. in Nanoengineering (Nanoscale Protein Engineering)
  - Ph.D. in AI/ML – Howard University (Causal Explainable AI)
  - Ph.D. in Information Technology – Towson University (Causal Explainable AI)

Research Experience

Computational Biology and Artificial Intelligence

- xD | U.S Census Bureau
  - Causality & Explainability for Fair & Trustworthy AI Systems.
- Center for Biologics Evaluation and Research, U.S Food & Drug Administration (FDA)
  - AI/ML for computational biology and drug discovery.
- U.S ARMY DEVCOM Army Research Laboratory
  - Causal Explainable Artificial Reasoning Systems.
- U.S. DoD Center of Excellence AI/ML - Howard University
  - Causal Explainable Artificial Reasoning Systems.
- Joint School of Nanoscience & Nanoengineering
  - Nanoscale Synthetic Proteins for Biomedical Applications.

Research Expertise & Publications

TOWSON UNIVERSITY

- Computational Biology.
  - Nanoscale Modeling and Simulations
  - Protein/Peptide Design and Engineering
  - Molecular Dynamics/Quantum Mechanical and Atomistic Modeling
  - Artificial Intelligence (AI) & Machine Learning (ML) for antibody design.
- Artificial Intelligence & Machine Learning
  - Explainable AI (XAI) for Robust AI Models
  - Causal Learning for Artificial Reasoning Systems.
  - Responsible & Trustworthy AI
- Google scholar for an updated publication list.
  - Peer reviewed Journals and Conference proceedings and a Book Chapter.

Cyber Foundations

Lesson 1: Overview

Student Learning Outcomes

Upon completion of this lesson, students will be able to:

- Describe what cybersecurity is and its importance
- Understand what we are protecting from attackers
- Understand the lessons learned from historical and current events, and emerging trends
- Describe the security principles and key terms, including the CIA triad
- Identify top threats and assess the likelihood of an attack
- Compare and contract approaches to network security

Introduction

Computer systems and networks are all around us

- Online banking
- Automated supermarket checkouts
- Online classes
- Online shopping
- Online travel resources
- E-Bay, Amazon, Half.com for textbooks
- Expedia, Travelocity, airplane e-tickets

From Smart People:

It's not what you don't know that will hurt you, it's what you know that ain't so.

Mark Twain

Too many unknowns, changing environment, cyber security is dynamic

Garbage times garbage is garbage squared.

Reed Augliere, security expert

If security is not done completely and properly, if only pay it lip service, there really is not security.

NO technology is 100% safe

Give humanity a technology and we will find a way to cheat; no technology is 100% safe.

Cyber security cannot be a check the box activity, it has to be structured and with a purpose.

Cyber Security must protect all of the company assets:

1. Personnel people are always number 1
2. Data
3. Hardware
4. Software

Cyber Security Facts:

- Digital assets now represent over 85% of an organizations value
- 99% of new information is stored digitally
- The average cost of a data breach in US today is $3.6 million (2017)
- The annual cost of cyber crime will top $8.8 trillion by 2022
- Cost of a breach of PII averages $148 PER RECORD, an increase of almost 5%
- Example: Facebooks collects an average of 15 terabytes daily

IBM Cost of a Breach Survey 2019 https://www.ibm.com/security/data-breach

Cyber Security Requires Resources but there are never enough

TOWSON UNIVERSITY

- 2019 Presidents Budget includes $15 billion for cyber security related activities, an increase of over 4% from 2018
- Cyber budgets are typically 5-7% of the IT budget
- The growth of the attack surface grows at a rate of over 600%, everything is interconnected
- You assume risk when you connect – Internet of Things (IOT), multifaceted
- Most devices have NOT embedded cyber security

IBM Cost of a Breach Survey 2019 https://www.ibm.com/security/data-breach

Breach Examples

- Every breach serves to raise awareness of the importance of cyber security and information privacy
- Facebook users information stolen = CEO Mar Zuckenberg testify before congress and Judiciary committees
- June 2017 Drug co Merck suffered a worldwide disruption of operations, hurt profits, cost insurance co $275M, biggest cyber insurance payout in history at that time.
- At least one in every 20 Fortune 1000 companies has experience a publicly disclosed breach (2017)
- Target’s security breach lost $1B (2015)
- Equifax loss of over 149M users’ data
- Yahoo data breach of 3M, decreasing value of company by $360M (was negotiating with Verizon for purchase)

What is Cybersecurity?

- The US Department of Defense (DoD) defines Cybersecurity as:

  “The **prevention** of damage to,
  protection of,
  and **restoration** of
  electronic systems
  to ensure its
  availability, integrity, authentication, confidentiality, and **nonrepudiation**.”

  (Source: DoDI 8500.01 Cybersecurity, 2014)

What is Cybersecurity?

Definition of *cybersecurity (Merriam-Webster)*

- measures taken to protect a computer or computer system against unauthorized access or attack

- Take Away
  - **Cybersecurity is the practice of protecting organizational assets from cyberattacks.**

Cyber Security began as a **Research Project**

- An experimental mobile program written in 1971 by Bob Thomas led to a computer program to move across a network leaving breadcrumb wherever it went; he named it CREEPER. As it moved through terminals it printed the message "I'M THE CREEPER: CATCH ME IF YOU CAN."
- Inventor of email, Ray Tomlinson, fiddled with the worm and made it self-replicating – creating the first worm program. Then he wrote the first antivirus software and named it REAPER. It tracked the CREEPER and deleted the crumbs it left.
- In the late 80's computer viruses became a serious threat.
- In 1988 Robert Morris wrote a program to program to across networks and infiltrate UNIS terminal using a KNOWN BUG, trying to draw attend that this bug existed and needed to be fixed. But Morris's program replicated so aggressively it seriously damaged critical networks, creating a Denial of Service attack. He was the first person convicted under the Computer Fraud and Abuse Act and led to the creation of the nation-wide Computer Emergency Response Team, the precursor to US CERT.
- Cyber Security was started as an information technology issue, not a security issue

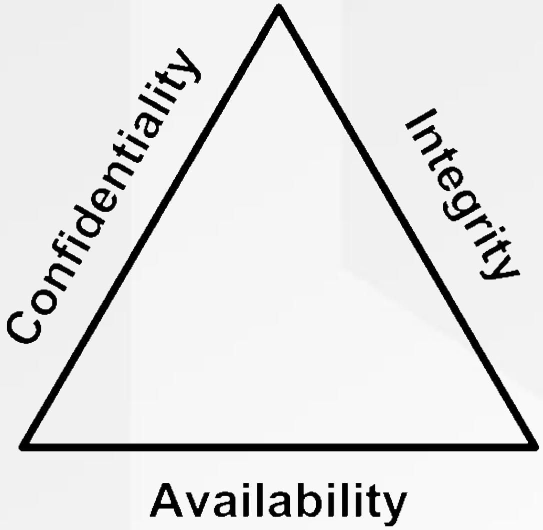
Historical Perspectives of Cybersecurity

- In the past few years, the cyber attacks have evolved from simple attacks created by script kiddies to nation-sponsored attacks compromising countries' elections

- Milestone events that had a major impact on cybersecurity
  - https://www.varonis.com/blog/events-that-changed-cybersecurity/

- World Biggest Data Breaches and Hacks (2004—Present)
  - https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

The CIA triad – The Cyber Security Backbone



- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **Integrity**
  - **Data integrity**: assures that information and programs are changed only in a specified and authorized manner
  - **System integrity**: Assures that a system performs its operations in unimpaired manner
- **Availability**: assure that systems works promptly and service is not denied to authorized users

CIA Exercise

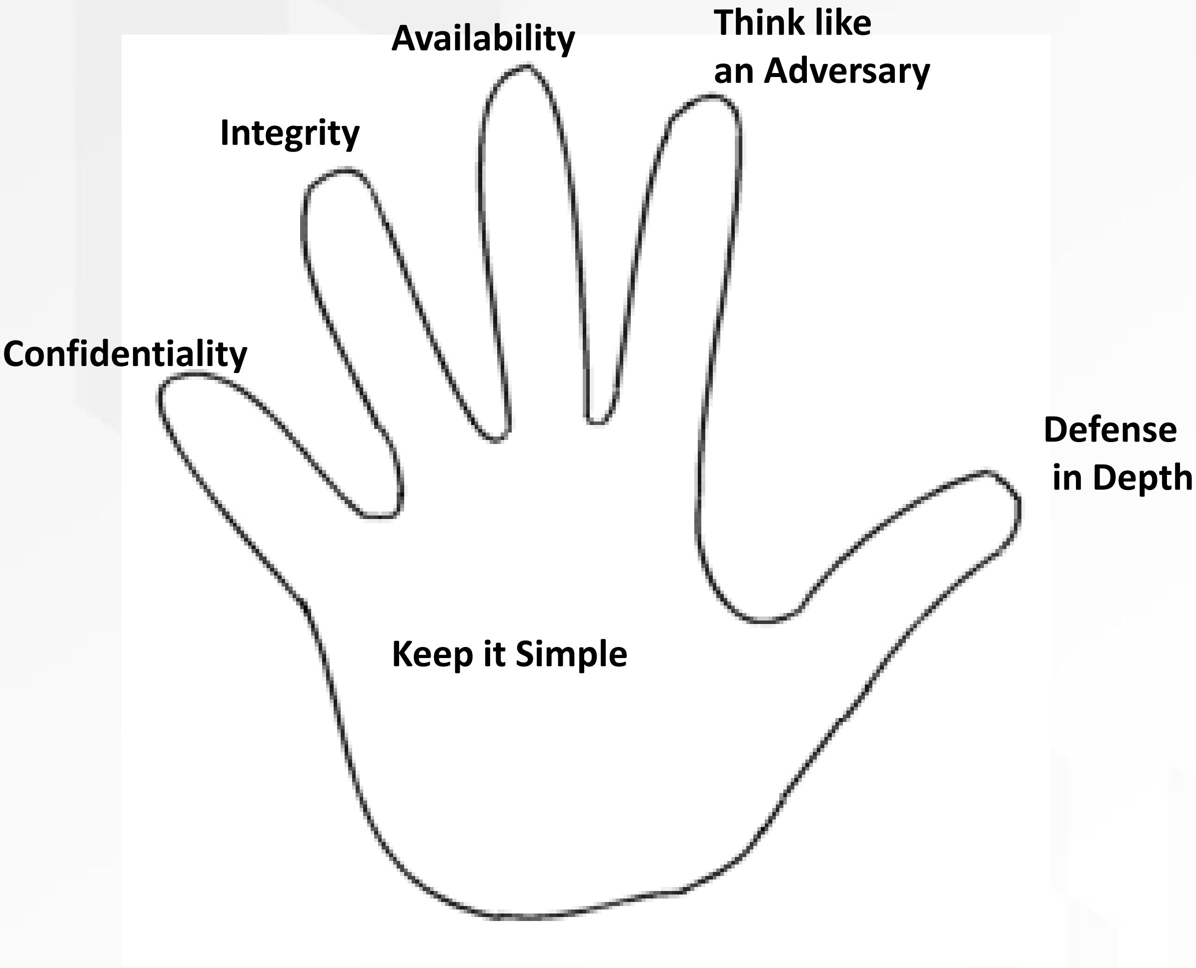
Match each statement with the relevant term of confidentiality, integrity and availability.

1. **Someone changed my Facebook profile photo without my knowledge.**

2. **I cannot print out my papers since I have no connection to the printer.**

3. **I need to encrypt my emails to prevent unauthorized access.**

Cyber Security Components for Protection



What are We Protecting?

- **Data:** Corporate and personnel information
- **Identity:** Someone’s personal information
  - The process by which the hackers steal someone’s personal information and use it without consent is called “Identity Theft”
- **Devices and Infrastructure:** Computing and network resources
  - Examples: Computers, Mobile Devices, Switches, Routers, etc.

Protecting Data

- Personally Identifiable Information (**PII**):
  - "Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name." (Source: NIST SP 800-122)
- Protected Health Information (**PHI**):
  - Medical information, Lab history, hospital records, medical insurance information, etc.
  - Financial Information: Billing, Banking, Credit Cards, etc
  - User Credentials: Username, Passwords, etc.
- Question: How can stolen data be used in a malicious manner?

Data: Most valuable organizational asset

- Examples: Trade Secrets, Business Plans, Customers and Employees Data, Research, etc.

- **Data at Rest:** Data that is stored in Media
- **Data in Transit (or in Motion):** Data transmitted from one location to other
- **Data in Use:** Data that is loaded in the computer Memory for processing

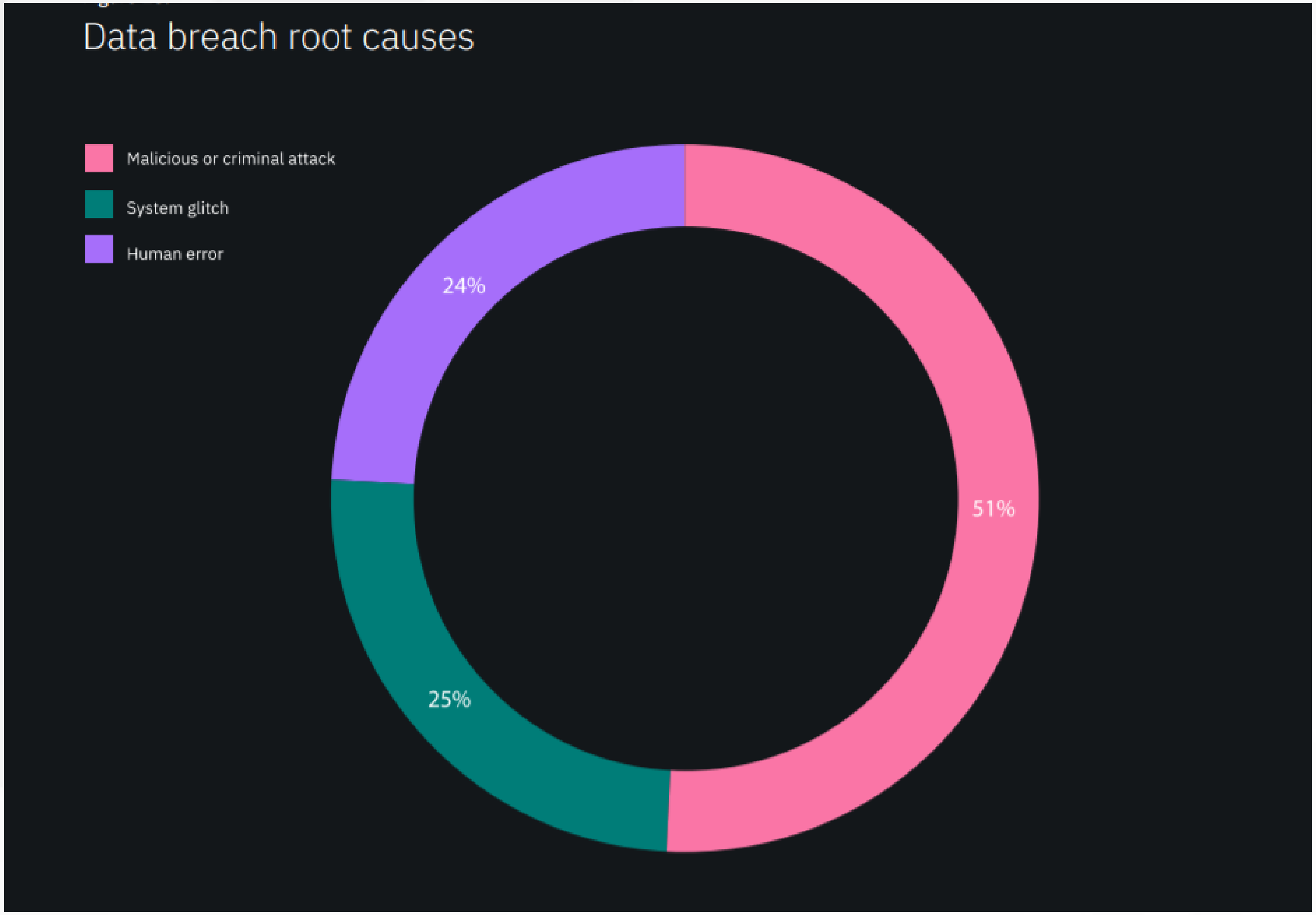
A Data/Network Breach

A data breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk, either in electronic or paper format.

There are three main causes of a data breach: malicious or criminal attack, system glitch or human error.

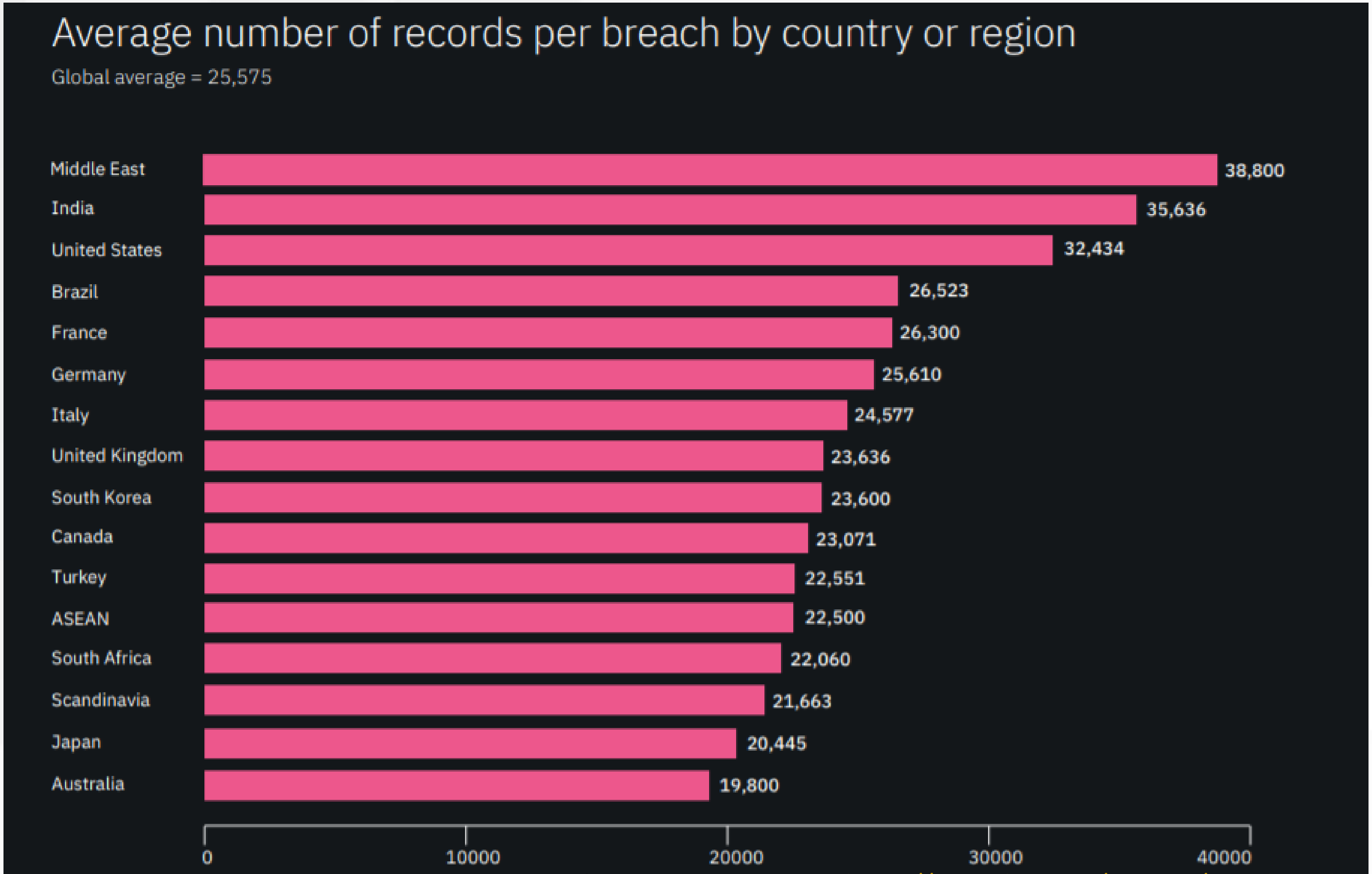
The costs of a data breach vary according to the cause and the safeguards in place at the time of the data breach

Top Breach Causes



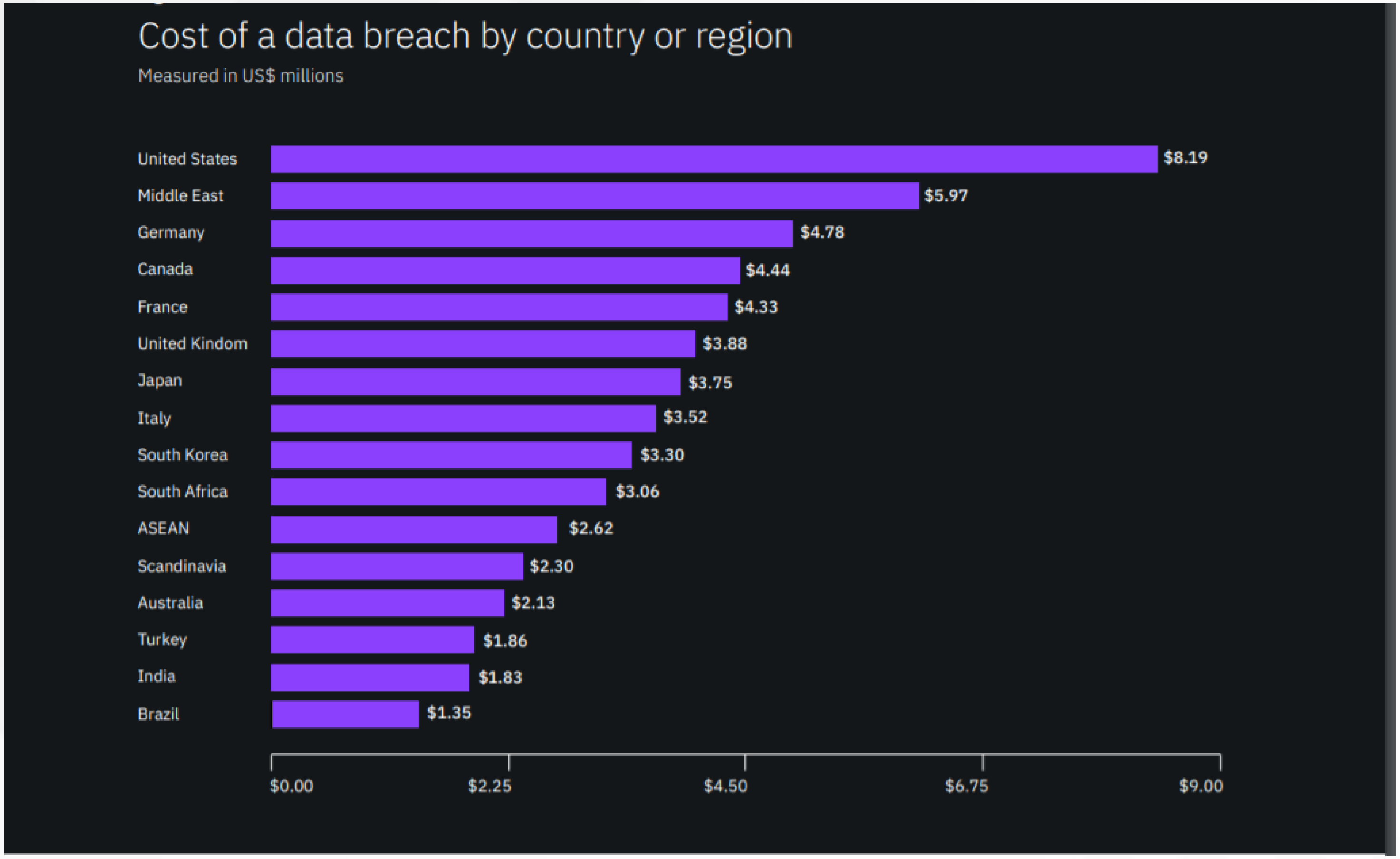
IBM Cost of a Breach Survey 2019 https://www.ibm.com/security/data-breach

One Breach Impacts Many



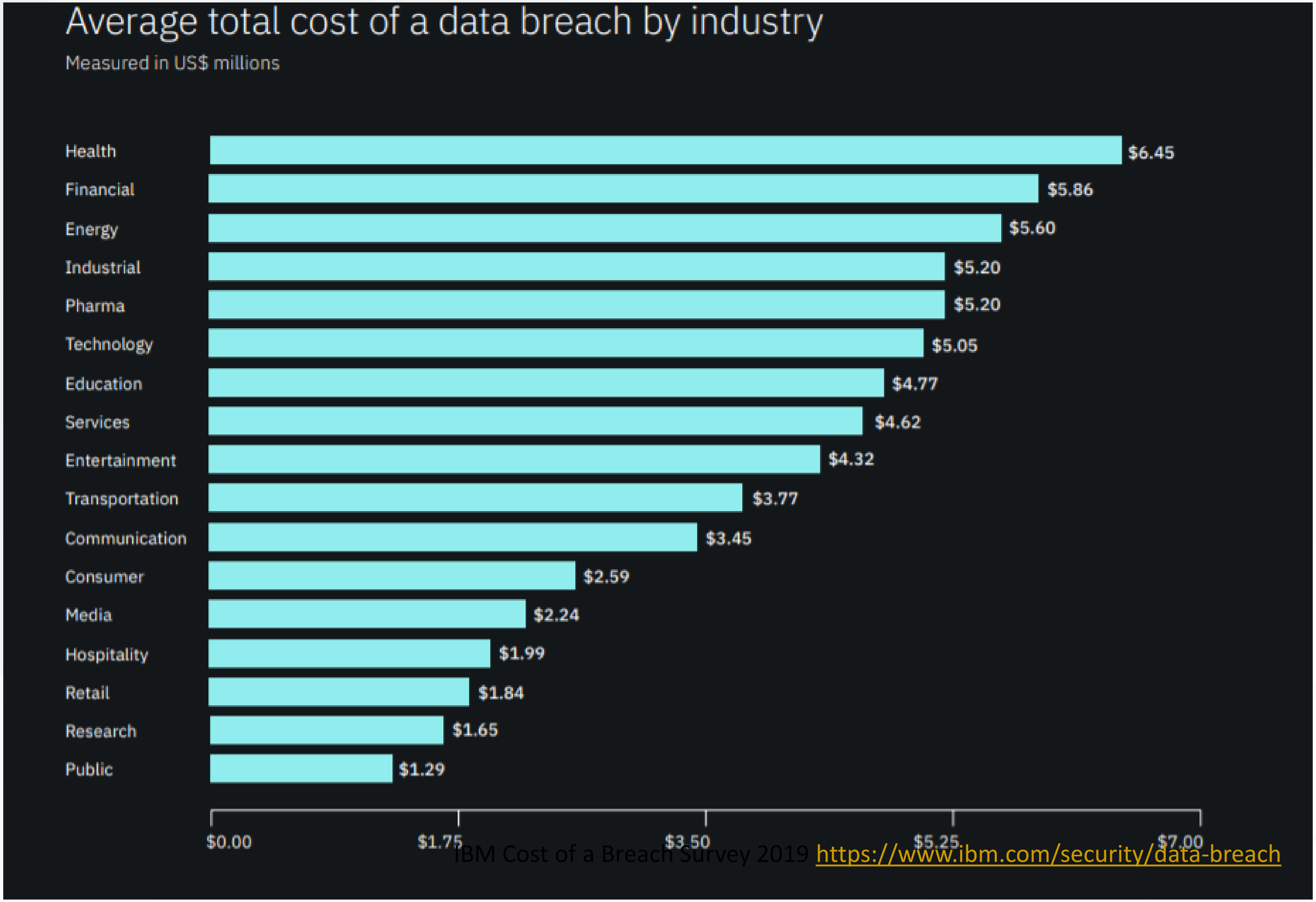
IBM Cost of a Breach Survey 2019 https://www.ibm.com/security/data-breach

Cost of a Data Breach Varies by Country



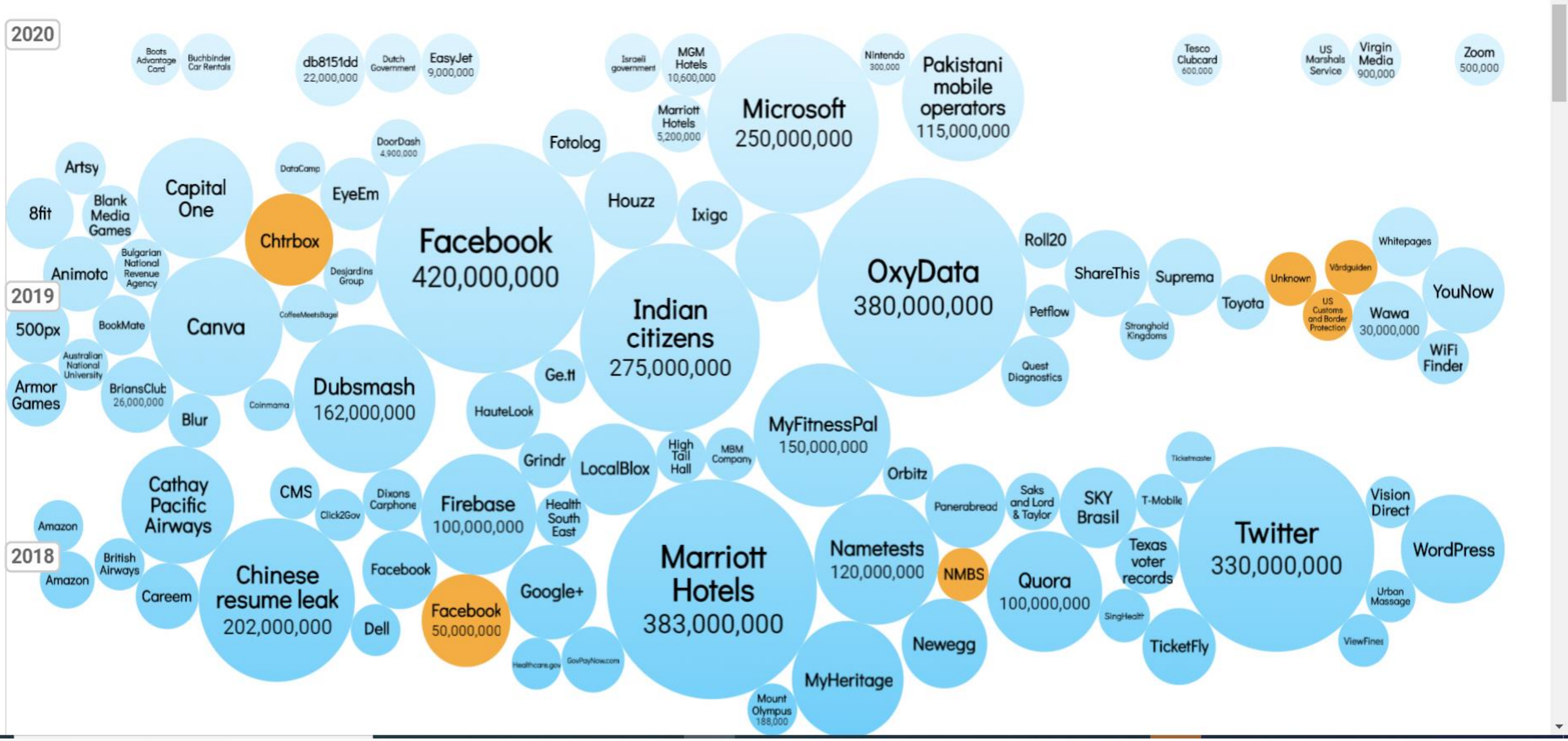
IBM Cost of a Breach Survey 2019 https://www.ibm.com/security/data-breach

Cost of Data Breach Varies by Industry



IBM Cost of a Breach Survey 2019 https://www.ibm.com/security/data-breach

Data Insecurity:



https://www.informationisbeautiful.net/

Breach Information

Figure 2. What tactics are utilized? (Actions)

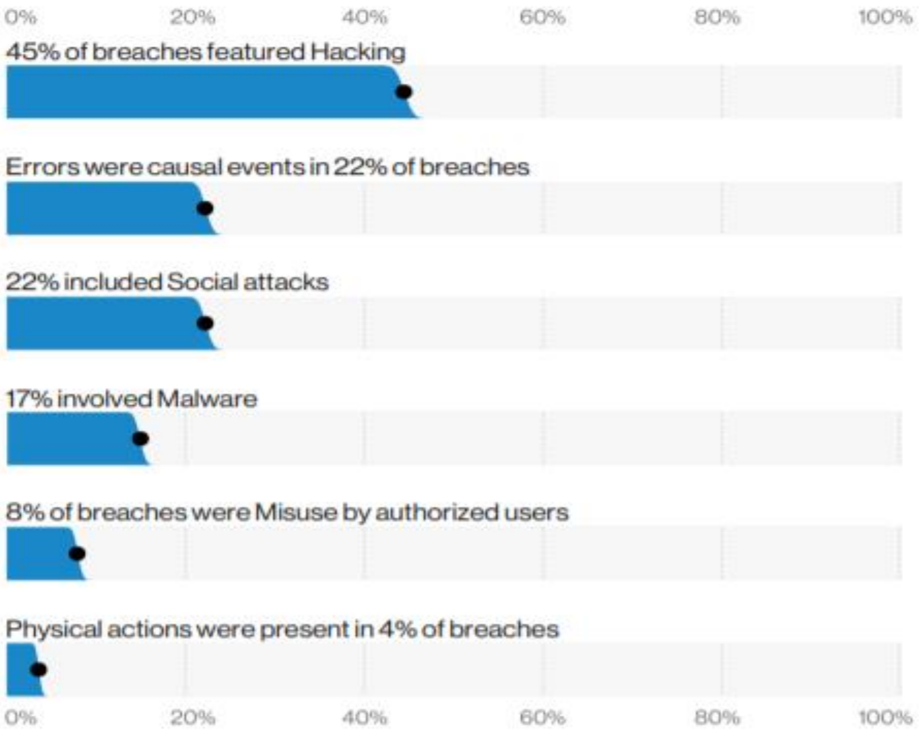
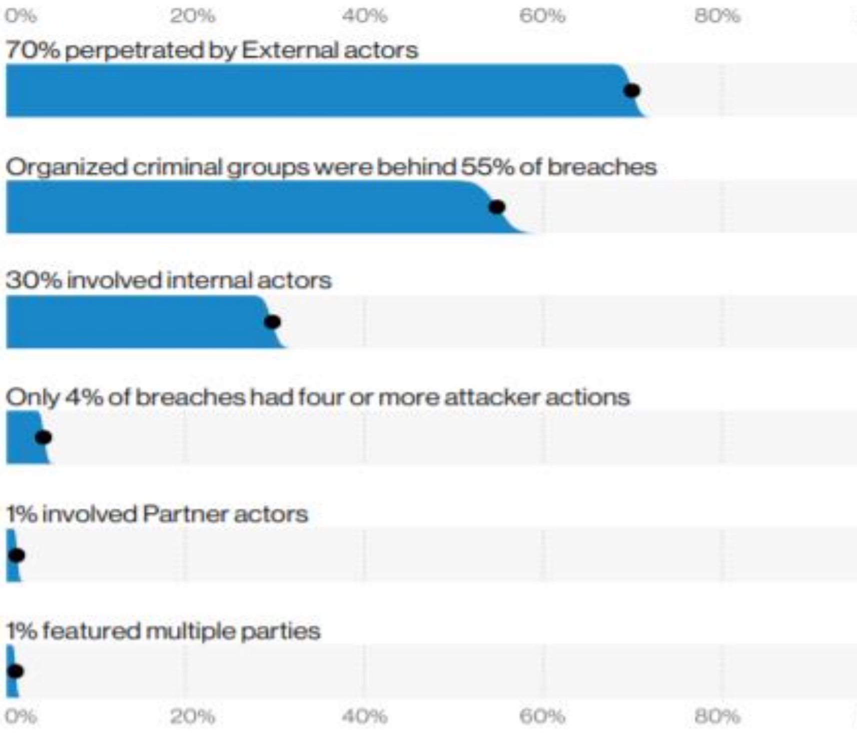


Figure 3. Who's behind the breaches?



https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf

Protect the Network: Critical Infrastructure

- **The Computer Security Act of 1987**
- **Presidential Decision Directive 63 (PDD-63): Protecting America's Critical Infrastructures (1998)**- outlines the increased reliance on cyber infrastructure by public and private enterprises, and the strong need for collaboration to improve the security of this infrastructure. The directive marked the first White House effort to address vulnerabilities from the United States dependence on cyberspace

Critical Infrastructure –the Value of your Network/Data

TOWSON UNIVERSITY

1. Chemical Sector
2. Communications Sector
3. Commercial Facilities Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Sector
16. Water and Wastewater Systems Sector

https://www.dhs.gov/cisa/critical-infrastructure-sectors

DISCUSSION - How Seriously Do You Take Threats to YOUR Network's Security?

Which group do you belong to?

- "No one is coming after me/my computer."
  - Prove to me that I am at risk
  - Ostrich Theory
- "The sky is falling!!"
  - Prove to me that I am not at risk
  - Paranoia
- Middle Ground
  - An educated awareness of true risk

Emerging Trends

- Cybersecurity is becoming more intelligence driven and automated
  - Artificial Intelligence (AI) based techniques are being used to improve operations and automate various tasks
- Organizations are more focused on cloud-based security platforms
  - Security-as-a-Service (SECaaS) is becoming common
- Growth and Diversity of Mobile Devices
  - Because of the disparate nature of these devices, it will be hard for organizations to deploy unified protection mechanisms
- Cryptojacking is on the rise
  - Organizations are already investing in cryptocurrency mining detectors to identify unauthorized usage of organizations' computing resources to mine virtual coins
- Better, Smarter IoT based Botnets will emerge
  - Because of large-scale compromises of unpatched routers and IoT

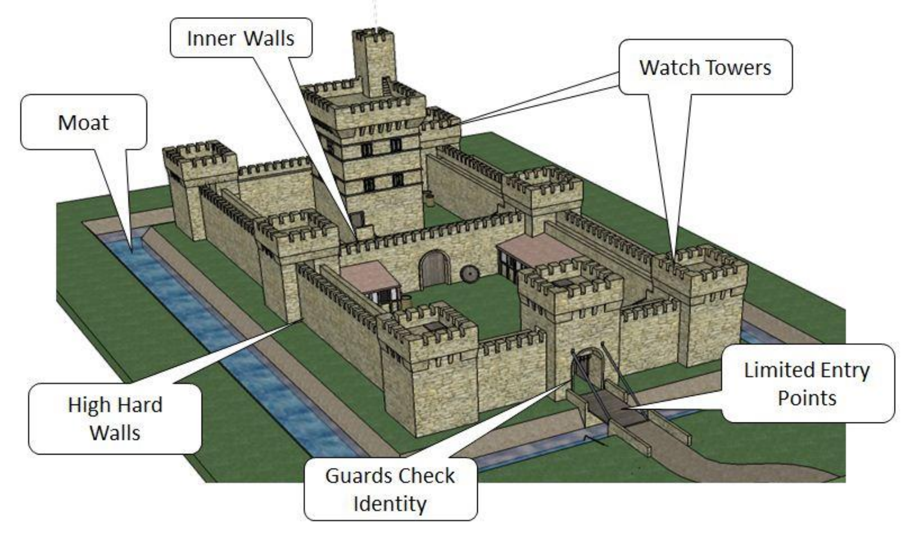
THINK LIKE AN ADVERSARY

Network Security Paradigms

- Perimeter security approach
  - Perimeter Defense is the most popular because it used to be clearly defined, but as companies hire mobile workers, home workers, and contract workers, the perimeter is becoming less and less clearly defined.
- Layered security approach
  - Not only the perimeter but separate sections of the network are protected to the security level assigned to them.
- Proactive Versus Reactive
  - Are your security measures active or passive?
  - Do you have a security plan, or are you part of someone else’s plan to intrude on you?
- Hybrid Security Method
  - Only a thorough and ongoing risk assessment and vulnerability can keep you informed about what combination of postures will benefit your network the most.

Defense in Depth

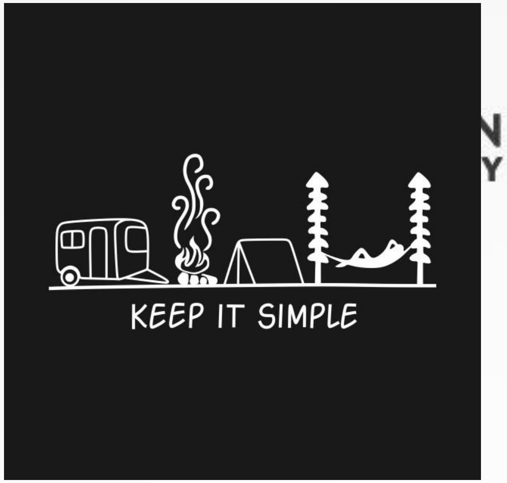
Abstraction
Layering
Modularity
Resource Encapsulation
Process Isolation
Domain Separation



Defense

- Most companies focus overwhelmingly on encryption and perimeter defense in a post-perimeter world to protect confidentiality. Their security plans undervalue availability, and rarely address integrity.
- Fortunately, important people are catching on. In testimony before Congress, James Clapper, the former director of national intelligence, said the biggest emerging threat to national security is "cyber operations that will change or manipulate electronic information in order to compromise its integrity instead of deleting or disrupting access to it."
- We can no longer count on keeping the hackers out. Let's work on ensuring we can catch them once they break in.

KEEP it simple (KISS)



- Minimization
- Simplicity
- “Complexity is the worst enemy of security,” (Bruce Schneier)
- easy-to-use and unified information security systems are going to be more effective because of their simplicity to roll out and manage.

Lessons Learned

- Anyone and everyone is susceptible when it comes to data breach
- Hackers have evolved so has the sophistication of their techniques
- The amount of attacks from overseas has increased drastically. This also includes state-sponsored attacks
- Insider threats are just as dangerous as outsiders
- Hackers are here to stay—It is a profitable business
- Attack on National Critical Infrastructure is imminent because of the inherent poor protection
- Advanced Persistent Threat (APT) and State-Sponsored groups will continue to attack with more sophistication

Summary

- Cyber security is a constantly changing field –it is DYNAMIC.
- You need to protect the data and the network
- Three critical concepts in cyber security: Confidentiality, Integrity, Availability, the CIA Triad.

Legal Constraints Impact Network Security

- *The Computer Security Act of 1987*
- *OMB Circular A-130*
- See www.alw.nih.gov/Security/FIRST/papers/legal/statelaw.txt for state computer laws
- Health Insurance Portability and Accountability Act of 1996, HIPAA

Online Resources Security Resources

- CERT-Computer Emergency Response Team, sponsored by Carnegie-Mellon University, the first computer incident response team
  - www.cert.org
- Microsoft Security Advisor – Microsoft security information, tools and updates
  - www.microsoft.com/security/default.mspx
- F-Secure – Information on virus outbreaks
  - www.f-secure.com
- SANS – Documentation on computer security issues
  - www.sans.org