CYBERSECURITY

NCPACA CONVENTION

FRIDAY, JULY 5, 2019
4:00-5:00 PM CST

MJ
McCONNELL & JONES LLP
CERTIFIED PUBLIC ACCOUNTANTS

Learning Objectives

At the end of this webinar, participants should be able to:

- Define what is cybersecurity.
- Learn about common types of cyber attacks.
- Understand what are the cybersecurity goals and how to implement them.

Sharjeel Ahsan, CPA

Senior Manager, ERISA Assurance and Compliance Services
McConnell & Jones LLP

Mr. Sharjeel Ahsan serves as an ERISA Assurance and Compliance Services Team Senior Manager and is responsible for managing numerous employee benefit plan audits. He is also responsible for overall project performance, including all aspects of managing the fieldwork, supervision of the audit team, and audit report review/compliance. Mr. Ahsan has extensive knowledge of accounting and technical reporting standards and has assisted clients with their annual audit and reporting requirements for both defined benefit and defined contribution plans as well as Form 5500 filings.

In addition, **Mr. Ahsan** leads the firm's form 5500 preparation practice and has helped several clients through DOL & IRS voluntary correction programs.

Mr. Ahsan has over 12 years of experience in accounting and financial audits for a variety of industries and employee benefit plans. He has planned and supervised numerous employee benefit plans, including defined contribution (401(a), 403(b), 401(k)) plans (including plans requiring Form 11-K filings), defined benefit (traditional pension and cash balance) plans, health and welfare plans with a section 401(h) arrangement, and master trust investment accounts. He has been on the McConnell & Jones LLP's ERISA Assurance and Compliance Services Team for more than 12 years. Mr. Ahsan participates in national webinars on Employee Benefit Plan topics and is a regular editorial contributor to the 401(k) Advisor, which is a monthly publication published by Wolters Kluwer.

Education / Certifications:

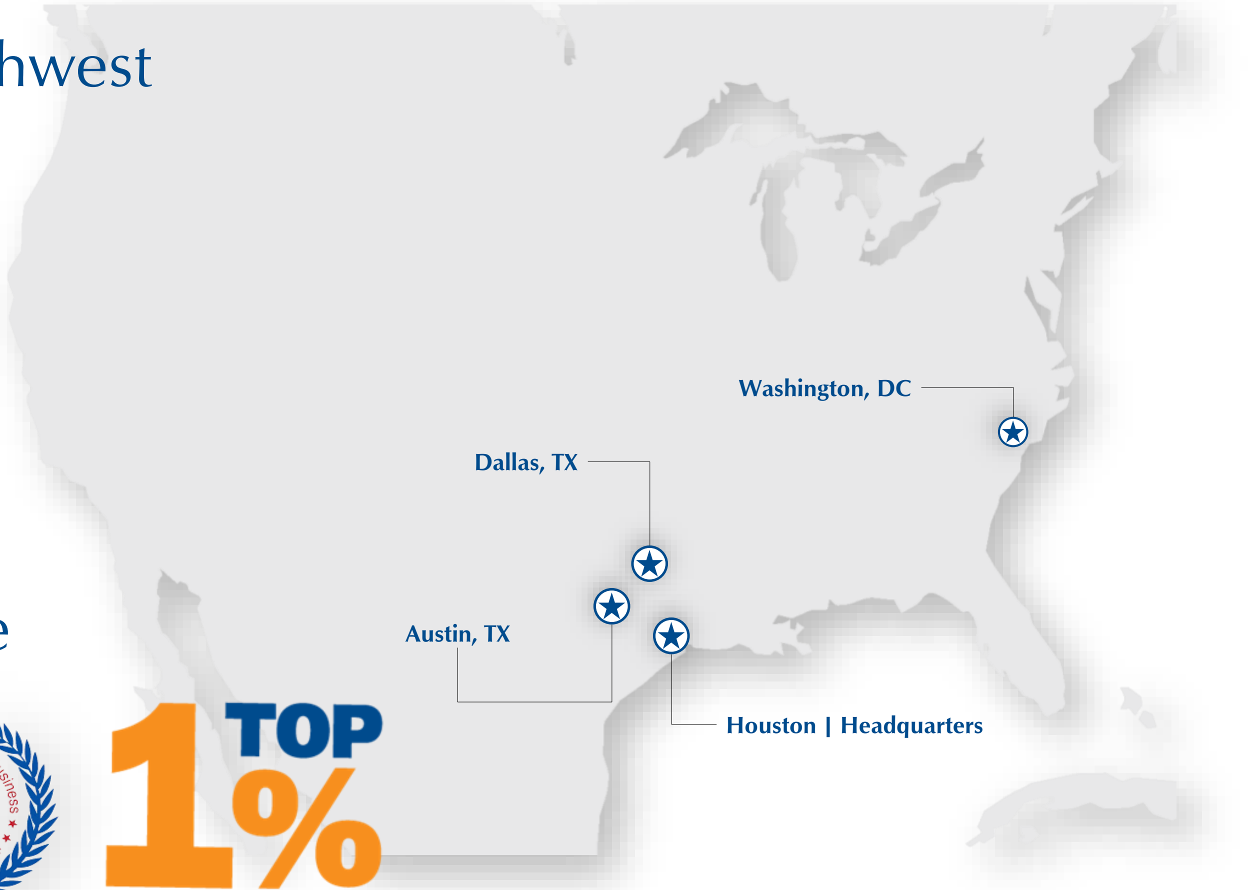
- MBA, Accounting and Finance, Nicholls State University
- BS, Accounting, University of the Punjab
- Certified Public Accountant

Member of:

- American Institute of Certified Public Accountants

About McConnell & Jones LLP

- Top 20 Accounting Firm in the Southwest *(Accounting Today)*
- Veteran Owned Small Business
- 100 + Employees Nationwide
- Comprehensive Services
- Nationally Recognized EBP Practice



TOP 20 ACCOUNTING FIRM IN THE SOUTHWEST

Veteran Owned Small Business VOSB CVE

TOP 1% of Employee Benefit Plan Audit Firms

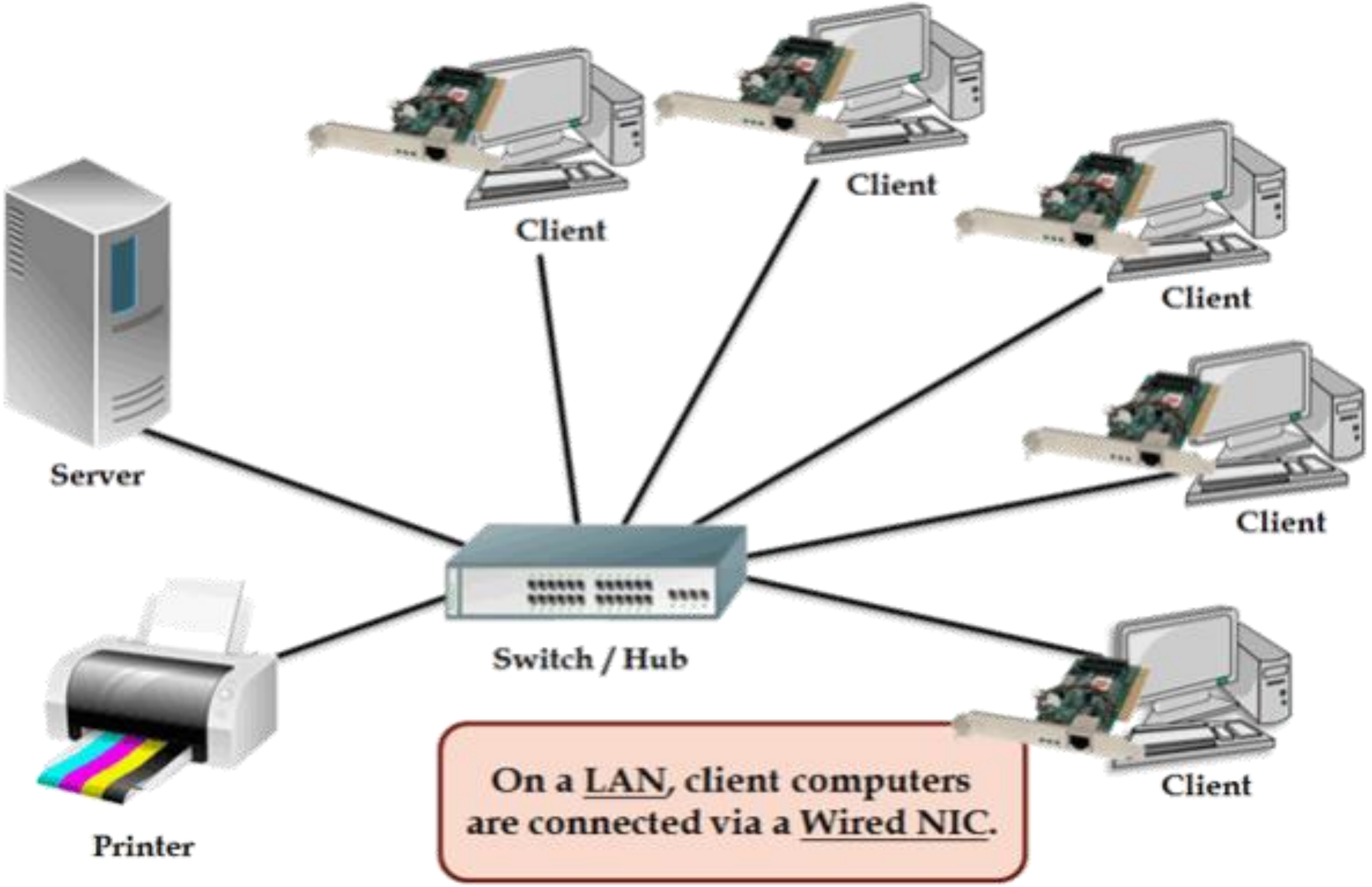
CYBERSECURITY

Historical Perspective

Main Frame Computers

Historical Perspective

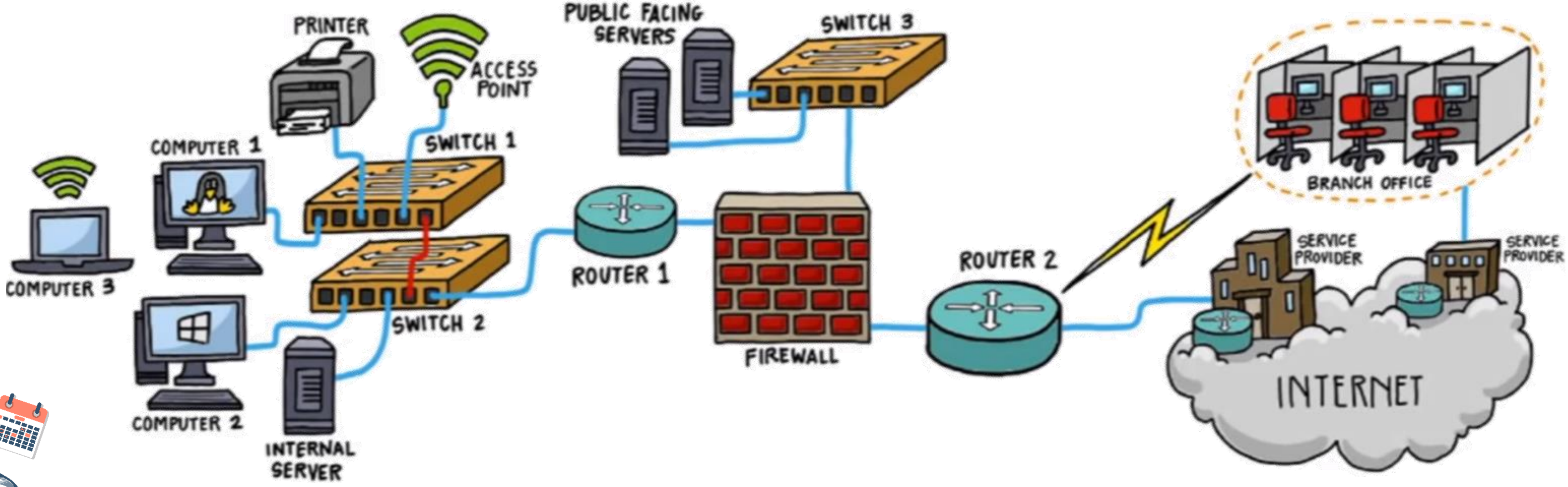
Wired Networked Computers



On a LAN, client computers are connected via a Wired NIC.

Historical Perspective

Internet / Wireless Networked Computers / WiFi



What is CYBERSECURITY?

CYBERSECURITY is...

- CYBERSECURITY is effectively protecting our systems, our networks, our applications from any kind of digital attack or compromise.
- It is the protection of internet-connected systems, including hardware, software and data, from cyber attacks.

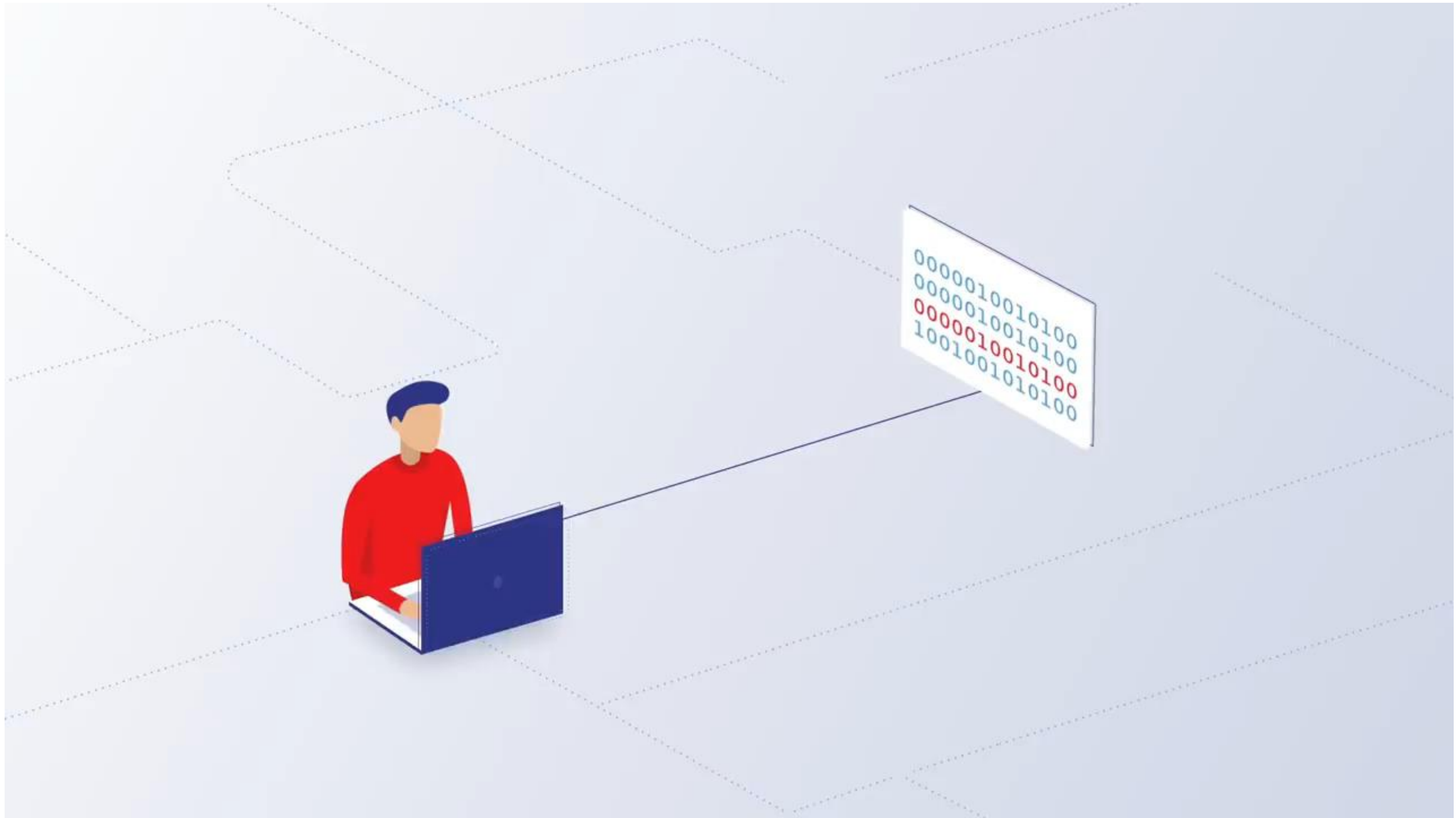
Why We Need CYBERSECURITY?

- Golden age for data exploits.
- It is so important because it is so expensive if there is compromise to our systems and to our networks and to our data.

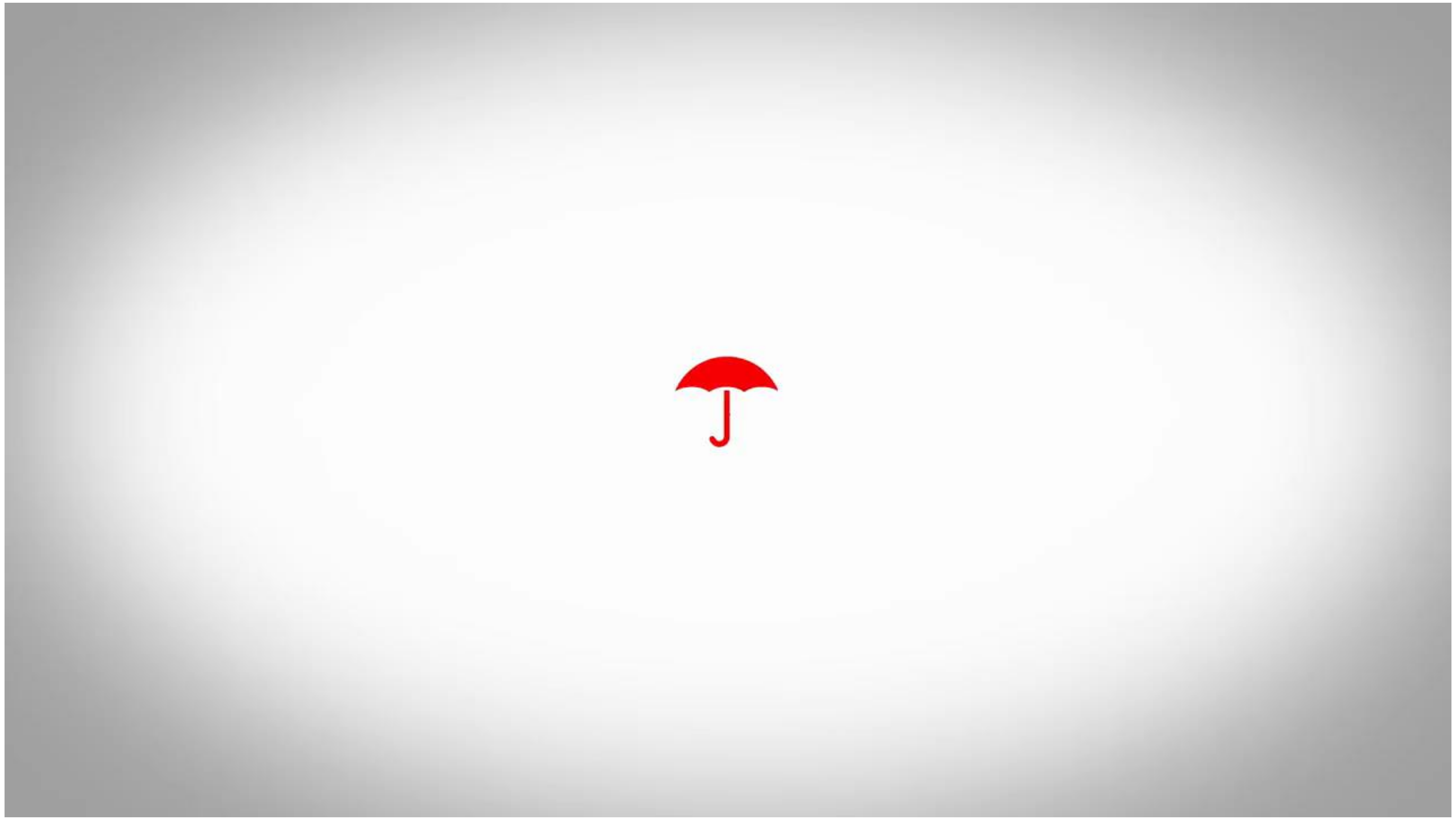
Estimated Cost

- Average data breach can cost a large enterprises an average of $4,000,000
- A destruction to a high volume commerce site may cost thousands of dollars of lost revenue each minute.
- Experts estimate that all cyber crimes will total $6 Trillion annually by 2021.

Two primary Weapons of Cyber Criminals



Five Types of Cyber Criminals



Five Types of Cyber Criminals

- The Social Engineer
- The Spear Phisher
- The Hacker
- The Rogue Employee
- The Ransom Artist

CYBERSECURITY Goals

CONFIDENTIALITY

- Secrecy or confidentiality, means that only authorized people should be able to access or read specific computer systems and data.

INTEGRITY

- Integrity means that only authorized people should have the ability to use or modify systems or data.

AVAILABILITY

- Availability means authorized people should always have access to their systems and data.

Security Goals

1. AUTHENTICATION

a. Only the people who are supposed to be able to access and see and modify the data should be able to do that

b. Can be achieved by Technical controls (e.g. 2 factor authentication)

2. AUTHORIZATION

a. Controlling what any individual is allowed to do

b. Defining Permissions and rights to access various resources

c. Preventing unauthorized access (Encryption)

Security Goals

3. HANDLING POTENTIAL COMPROMISE AND ATTACKS

a. Actions before attack

b. Actions during attack

c. Actions after attack

CYBERSECURITY Principles

CONFIDENTIALITY

≈ Cracking encrypted data

≈ Man in the middle attacks on plain text

≈ Data leakage / unauthorized copying of sensitive data

≈ Installing spyware / malware on a server

INTEGRITY

≈ Web penetration for malware insertion

≈ Maliciously accessing servers and forging records

≈ Unauthorized database scans

≈ Remotely controlling zombie systems

AVAILABILITY

≈ DOS/DDoS attacks

≈ Ransomware attacks – forced encryption of key data

≈ Deliberately disrupting a server rooms power supply

≈ Flooding a server with too many questions

Four Laws of CYBERSECURITY

1. If there is a vulnerability, it will be exploited
2. Everything is vulnerable in some way
3. Humans trust even when they should not
4. With innovations, comes opportunity for exploitations

Questions & Answers

We're Here For You

Sharjeel Ahsan, CPA
Senior Manager

Telephone – 713.968.1689
SAhsan@mjlm.com

...and follow McConnell & Jones LLP online:

- www.mcconnelljones.com
- https://www.facebook.com/mcconnellandjonesllp/
- httpas://twitter.com/mj_cpa
- https://www.linkedin.com/company/1222367/