APPARELIST

Cyber Security

Clients First® BUSINESS SOLUTIONS

PRINTING UNITED ALLIANCE

Agenda

- Introductions
- Statistics
- Cyber Security 101 - How to Protect your Company and your Clients
  - Building your Cyber Security Defenses
- Cyber Security and the Human Condition
- Internet of Things (IoT) - the role this plays
- AI and the impact on Cyber Security
- Cyber Security Roadmap
- Q & A

Who can tell me…

- 2,900,000,000 (2.9 Billion) — The number of rows of personal data taken from the National Public Data breach (estimated to impact over 137 million US citizens)
- 1,700,000,000,000 (1.7 Trillion) — The number of times hackers attempt to get into Microsoft networks last year
- 4,000,000,000,000 (4 Trillion) — The size of file (4TB) taken from the National Public Data breach

Hackers, Malicious(Bad) Actors are not stopping

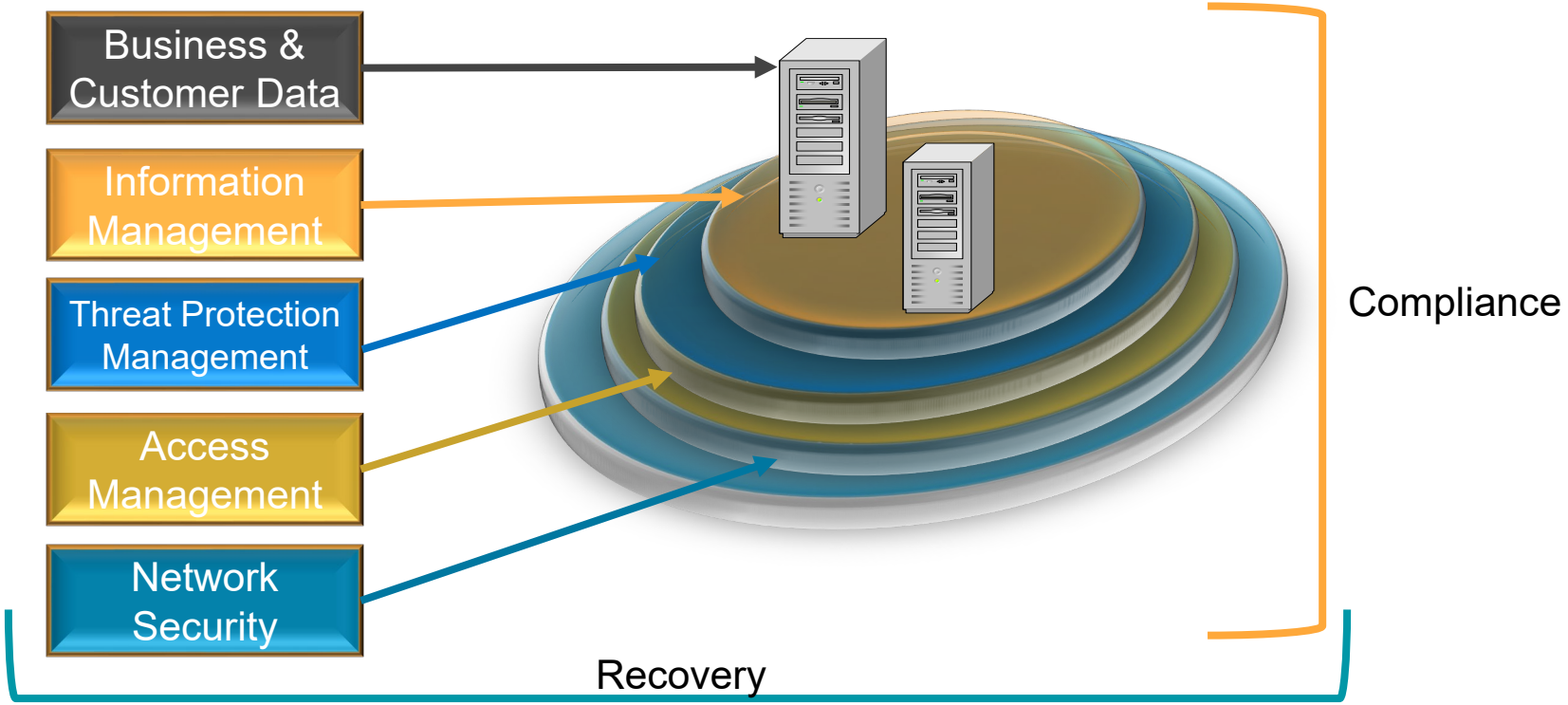
- According to the FBI
  - Hackers make more money on smaller company
    - This may be you, your suppliers, or your customers
  - 350% increase since 2020
- 46 The percentage of all Cyber breaches against companies with fewer that 1,000 employees (in 2021)
- 95 The percentage of all Cyber attacks in the US that are focused on small business (95%, in 2023/24)
- 50,000 The average ransom paid by small business to get back their data, their systems
- 1 in 3 The odds that after paying the ransom you can recover your data 33%

Clients First® BUSINESS SOLUTIONS

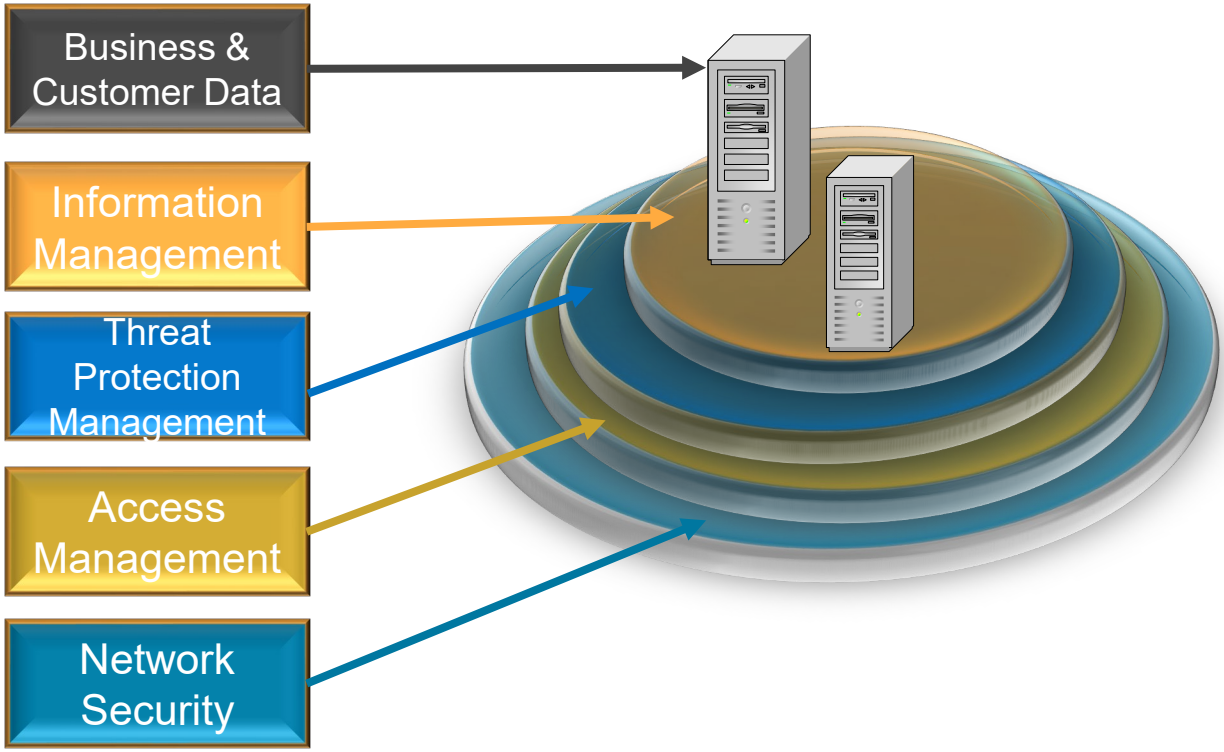
Protect the data you are handling

- Understand the type of data that is on your machine/server(s)
- Avoid storing PII data (personally identifiable information)
- Pay attention when you have to email sensitive information

How to protect your company and your clients



Cybersecurity Model – Information: High-Trust, MIS/ERP Data, Customer Files (is it backed-up? Immutable? Recoverable?)



Information Management:
(Basic) Data Back-up
(Advanced) Validated Back-up and Recovery

Threat Protection Management:
(Basic) Virus Protection
(Advanced) Password Protection, Anti-Phishing, Penetration testing

Access Management:
(Basic) Password Expiration
(Advanced) SSO, Multi-Factor Authentication

Network Security:
(Basic) Firewall
(Advanced) 24/ 7 Active Monitoring

Compliance

- Vigilance
  - Continuous training, adherence, forced changes based upon predefined intervals
- Review, Correct, Repeat
- Tools
  - Password manager software
  - Password rotation
  - Simulated Phishing and review
  - Vulnerability scanning and review
  - Penetration Testing and review

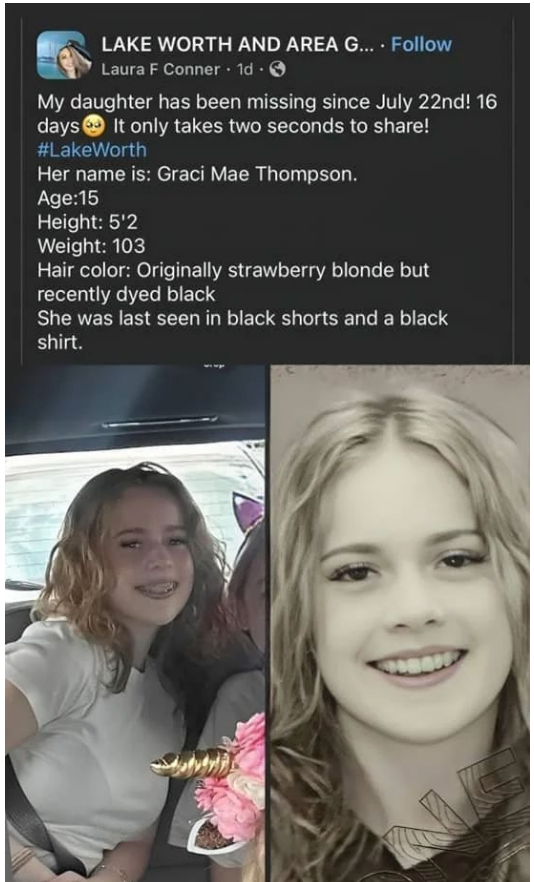
Recovery

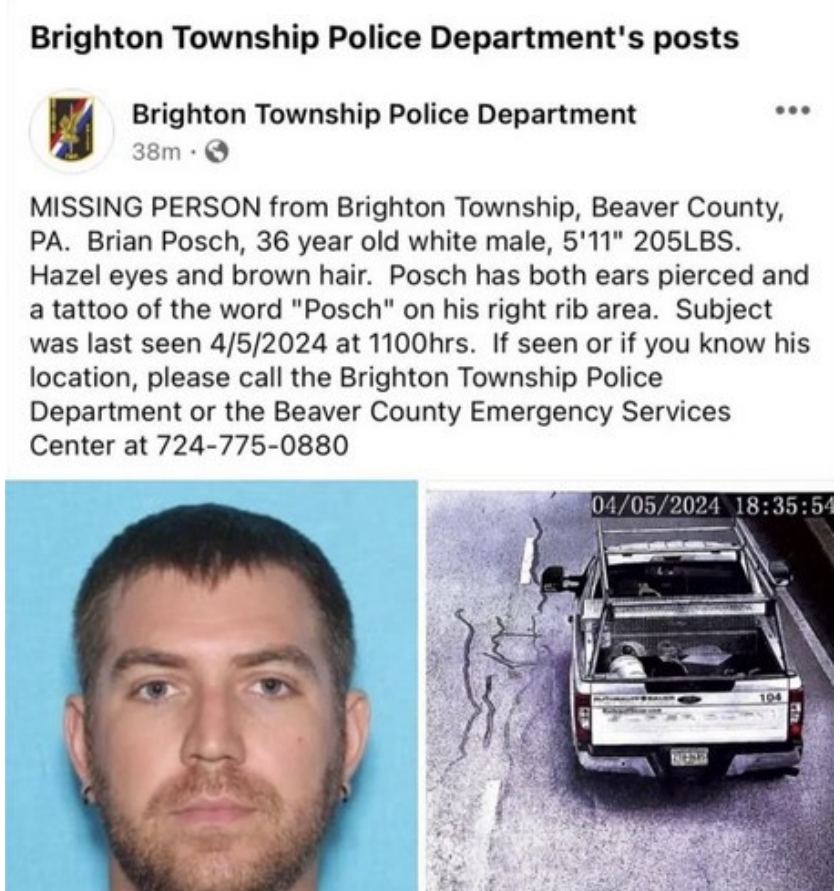
- Vigilance
  - Do you perform robust back-ups? 15 min. intervals?
    - On-Premise Applications
    - Cloud applications
- Are your servers virtualized?
  - Does your back-ups include virtualization of the server environment
- Are your backups immutable?
- Are your back-ups
  - Inverse Chain? Or Incremental?

Cyber Security and the Human condition

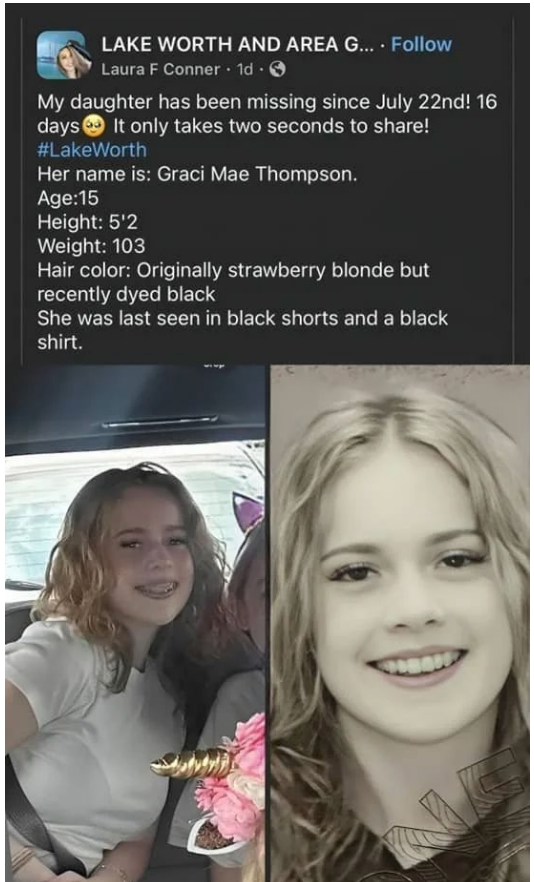
- Who has heard of?
  - Gracie Mae Thompson
  - Brian Posch

Cyber Security and The Human condition





Cyber Security and The Human condition



Fake / Scam

If you click on the links, or offered to volunteer a virus is being downloaded onto your computer

Clients First® BUSINESS SOLUTIONS

Cyber Security and The Human condition

Brighton Township Police Department's posts

Brighton Township Police Department
38m ·

MISSING PERSON from Brighton Township, Beaver County, PA. Brian Posch, 36 year old white male, 5'11" 205LBS. Hazel eyes and brown hair. Posch has both ears pierced and a tattoo of the word "Posch" on his right rib area. Subject was last seen 4/5/2024 at 1100hrs. If seen or if you know his location, please call the Brighton Township Police Department or the Beaver County Emergency Services Center at 724-775-0880

In April, this was a real post. Unfortunately he was found deceased 4 days later submerged within his truck in a river

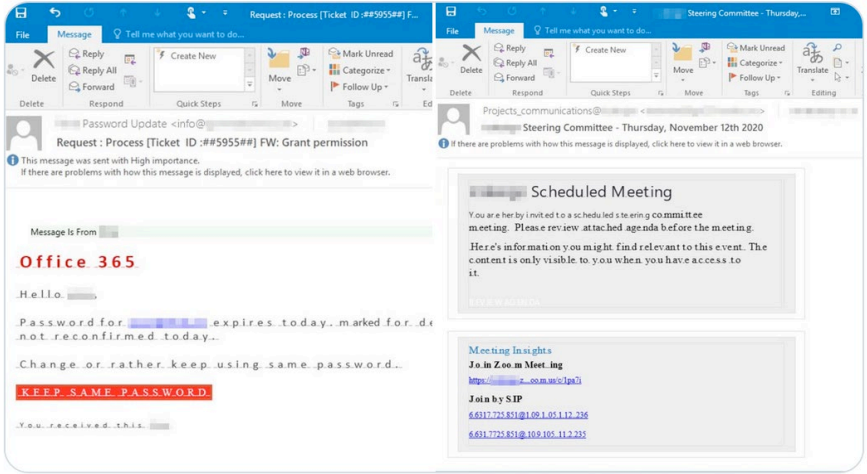
Since July over 20 different versions are on social media asking for help and volunteers

If you click on the links, your computer is being infected with a virus

Cyber Security and the Human Condition

Microsoft Security Intelligence ✓
@MsftSecIntel

We're tracking an active credential phishing attack targeting enterprises that uses multiple sophisticated methods for defense evasion and social engineering. The campaign uses timely lures relevant to remote work, like password updates, conferencing info, helpdesk tickets, etc.



Social engineered emails that create:

A Sense of urgency

1. A request for help (e.g. Helpdesk/ support)
2. Password reset
3. A meeting that you need to attend
4. Senior manager asking you to do something for them

Mailbox capacity for tfalteich@clientsfirst-us.com has exceeded its limit.

M

MS* | Webservices <info@aiikuen.com>
To Thomas Falteich

Reply | Reply All | Forward

Wed 11/15/2023 2:33 PM

Dynamics CRM

+ Get more add-ins

EMAIL SECURITY

Warning: Sender info@aiikuen.com has never sent any emails to your organization.
Please be careful before replying or clicking on the URLs.

Report As Malicious Report As Safe

powered by

Microsoft

The quota limit of your email is nearly full.

90% Used

86.40GB used. At 96.00GB you won't be able to send emails.

To prevent your **Incoming/Outgoing** mail from getting errors

Clear Cache Now

Microsoft Postmaster Delivery System Team

MS Corporation, One MS Way, Redmond, WA 98052

Cyber Security and the Human condition

- Quishing
  - QR Codes that are used for phishing attacks
  - When clicking the QR code
    - Malware can be downloaded (granting full access of your phone's data)
    - or a fake prompt with a sense of "urgency" to have an end user enter account data

Microsoft

Microsoft Multi-factor Authentication 2FA Set up.

Your 2FA multi-factor settings requires review. Follow the steps below to review and verify.
Quickly scan the QR Code below with your smartphone camera to re-authenticate your password security.

1. Scan the Microsoft QR Code using your phone camera.
2. Access your account, then go to settings.
3. Review and verify contact information and click save changes.

Cyber Security and the Human condition

- smishing
  - SMS (Text) phishing attacks
  - A social engineering attack that uses fake mobile text messages
  - When clicking the link
    - Malware can be downloaded (granting the ability to share your phone's data)
    - or tricked into sending money
  - Recent examples:
    - April, 2024 The FBI issued and alert for text messages coming from Toll agencies claiming unpaid tolls.
    - June, 2024 text messages from shipping companies like FedEx, UPS, USPS claiming a problem with your delivery to either please pay the additional shipping cost or "sign" online to receive the package

Cyber Security and the Human condition

- Why is this important
  - How many spam emails are sent **daily?**
    - 15 Billion is the current estimate as of
  - According to the latest release of:
    - 2024 Data Breach Investigation Report (DBIR)
  - 14% of Breaches involved exploitations of infrastructure
    - 300% increase (year over year)
  - 68% of breaches involved a non-malicious human element
    - Someone fell victim to a social engineering attack
    - Someone clicked a link on an email, a text message, a QR code
    - Someone made an error
      - Saving their Passwords in their browser

Cyber Security and the Internet of Things (IoT)

- Why is this important
  - According to Cisco, there will be over 75 billion devices connected to the internet by the end of 2025
  - When conducting a Vulnerability or Penetration Test make sure that all IP address types are in the plan
  - A few recent cyber hacks and where they virus was located
    - The IP based Security cameras for a manufacturing facility
    - The Document storage folder within a networked copier at a HQ facility
- Machine / Press integration – JDF/JMF - involves connecting multiple systems, such as ERP/MIS, RIPs, and production equipment
  - Each integration point can be a potential vulnerability, making it essential to regularly assess and patch these systems to protect against exploits

AI and Cyber Security

- The integration of AI in cyber security represents a dynamic shift in how organizations defend against evolving threats.
- AI is employed to enhance detection, response and prevention capabilities.
- Where AI can help us sniff out bad actors, it is also vulnerable to cyber attacks.
- Types of AI attacks:
  - Adversarial
  - Deep Fakes
  - AI-Powered Malware

AI and Cyber Security

- Adversarial
  - Purposeful manipulation – attackers purposefully manipulate input data to deceive machine learning models (i.e. make incorrect predictions / forecasting)
  - Evasion and misclassification – help attackers evade detection causing misclassification (i.e. adding noise to images, produce inaccurate results / design)
  - Continuous cat-and-mouse – when defenders and attackers play cat and mouse

AI and Cyber Security

- Deep Fakes – pose as a substantial

Threat by leveraging AI to create realistic,

Manipulated content

- Underscores the critical need for advanced

Detection and mitigation measures

- Organizations risk brand damage,

Financial losses and erosion of public trust

AI and Cyber Security

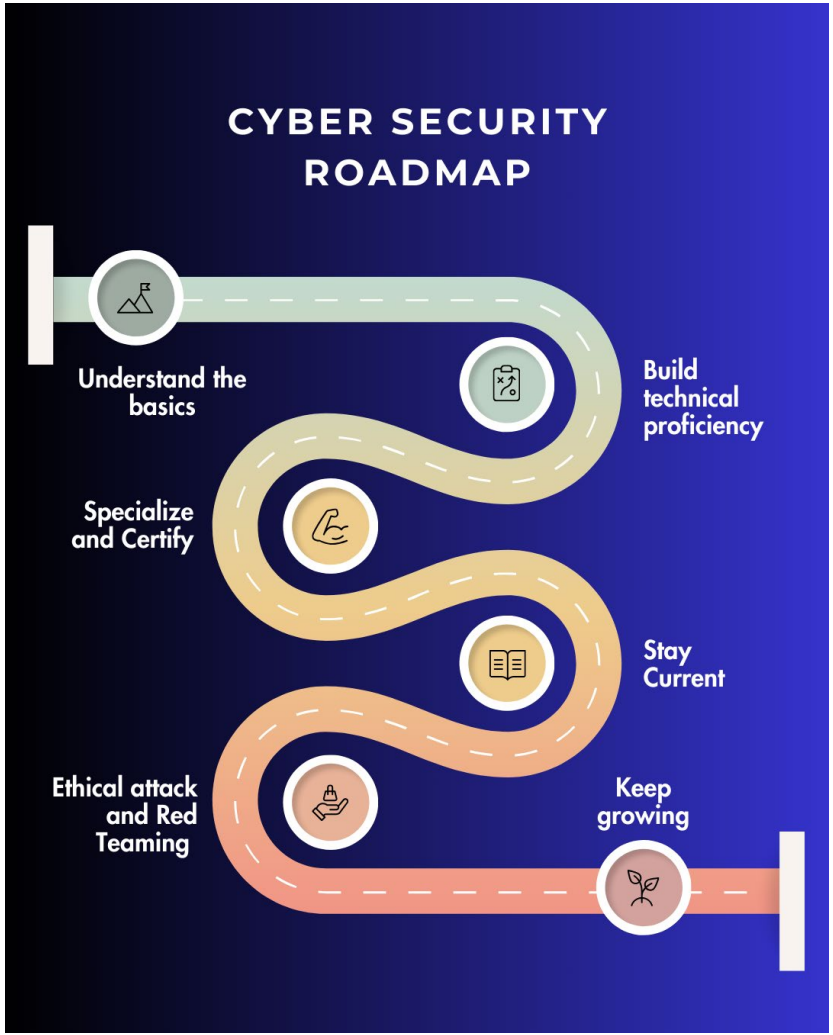
- AI Powered Malware – scariest of them all.....represents a paradigm shift in cyber threats. Infused with AI capabilities, this malware adapts, learns and evolves making it highly sophisticated and hard to detect.
- Its autonomous nature requires advanced

defense strategies

Cyber Security Roadmap

- Identify (Risk Identification)
  - Recognize vulnerabilities
  - Conduct a risk assessment
- Assess (Risk Assessment & Analysis)
  - Evaluate identified risks
  - Prioritize risks based on significance
- Mitigate (Risk Mitigation & Control)
  - Develop Strategies
  - Implement control
  - Conduct regular assessments (Compliance)
  - Address Gaps
- Monitor (Monitoring & Review)
  - Continuously Monitor (review the reports, make corrective actions)
  - Adapt to evolving threats

- **Lay the foundation** - learn, dive into fundamentals, explore concepts
- **Make sure your IT personnel is proficient** at the following:
  - Identify Risk
  - Assessing Risk
  - Mitigating Risk
  - Monitoring Risk
- **Specialize and Certify** – Hands on Practice within your IT teams and certifications of your staff
- **Stay Current** – Threat Intelligence
  - Keep an eye on emerging trends
  - Understand threat actors and their tactics
- **Ethical Hacking**
  - Penetration tests
  - Simulate real-world attacks



Where do you go from here?

- Begin or evaluate your current Cyber Security Plan
- Validate your Back-up and Recovery Strategy
- Schedule a Vulnerability or Penetration Test
- Identify your risks, and potential layered security
- Implement Control
- Train
- Continuously improve (Compliance)

Clients First® BUSINESS SOLUTIONS

Questions?

Thomas Falteich
tfalteich@clientsfirst-us.com

Amy Servi
aservi@clientsfirst-us.com

Your Best Interest is Our Purpose