About Me

GREG TOMCHICK
CEO, Valor Cybersecurity

- **Local Roots** → Pro Baseball

- **Software Company Founder** → Cyber Attack Victim

- **Building Expertise** → Defense Contracting, Navigant (Private Sector), early employee at Cyber Defense Labs.

- Founded **Valor Cybersecurity** in 2021.

- Focused on empowering business leaders to implement cybersecurity best practices.

What would happen if your business caught fire tomorrow?.......

Home Business Landscape

- Business data is being processed on the same connection as other high-risk activities (streaming, smart home devices, etc.)

- Personal mobile devices are being used for business activities

- Cyber criminals attacking our supply chain (vendors)

- Government requirements are increasing

- Cyber Insurance isn't guaranteed

- Most SMBs do not have a cybersecurity strategy

- Average cost of a breach is **$110,000**

- No one is **100% secure**

Tabletop Exercise

01 What 3 vendors or systems do you rely upon to operate?

02 Do you know where your sensitive business sits? (i.e. employee, customer records, accounting files, etc.)

03 What could be the impact of an information theft or breach? (time, money, data,..)

04 What is your business doing to protect your assets? (IP, customer lists, bank accounts, etc.)

05 Are plans in place, and tested to restore your business operations?

Cybersecurity Best Practices

For Individuals

- Operate with a cybersafe mindset **(THINK BEFORE YOU CLICK)**
  - Trust your Gut, if it looks too good to be true it probably is!
- Watch security awareness videos when able to stay up to date on what an attack might look like and how to not be a victim
- Talk to your families about how you protect what is important
- Avoid Public Wi-Fi whenever possible
- Put Multi-Factor Authentication (MFA) in place for important accounts
- Update your devices/Delete unused 'Apps'
- Avoid making social media connections with strangers
- Turn off Apple Air Drop and Bluetooth when not in use
- Never store your passwords in an unsecured manner (Don't write them down on devices, share them with others, or place them in Word/Excel documents)
- Reduce what you put on social media, attackers love free knowledge!

Cybersecurity Best Practices

VALOR CYBERSECURITY

For Businesses

- Proactively assess the risks to your business and identify what is most important to keep the doors open (systems, data, and IP).

- Ask tough questions from your vendors
    - "As a customer, how are you protecting my data?"
    - Who owns my data? Who can access it?

- Encourage good cyber hygiene practices:
    - Locking unattended devices
    - Creating strong passwords
    - Implementing multi-factor authentication (MFA)
    - Avoiding public wi-fi when possible
    - Installing AV on all

- Put Policies and Response Plans in place and test them

- Consider Cyber Insurance Protections
    - It may be tough to get, but the longer your wait the more you may pay

- Talk to your people about how you protect what is important and make it apart of your culture. **Security Champions are key.**

THANK YOU

WWW.VALOR-CYBERSECURITY.COM

Reach out to us: info@valor-cybersecurity.com

400 Granby St. Norfolk, VA

(757) 276-8412