WISPA CTO / SECURITY

Cyber Security doesn't have to be a bad word.

Let's chat about how to up your game for your customers, employees and community at large.

John Brown, CISSP, CFI, CP-AMEL

- Been connected to the "net" since early 1980's
- Senior Security Evangelist for TEAM CYMRU
- 35+ years in software and network engineering
- Principal Technical Engineer for ICANN L-Root DNS
- Have built internet on 3 continents
- Past instructor for ISC2 (CISSP),
    - Mikrotik (MTCNA, CRE, CINE)
- Passionate about helping ISP's

What we will discuss

- **Laws and Rules**
  - Federal laws
  - State laws
  - Industry Rules, contract terms

- **Why you should care**
  - Protecting your Employees
  - Protecting your Customers
  - Protecting your business
  - Being a good Citizen / Netizen

What we will discuss

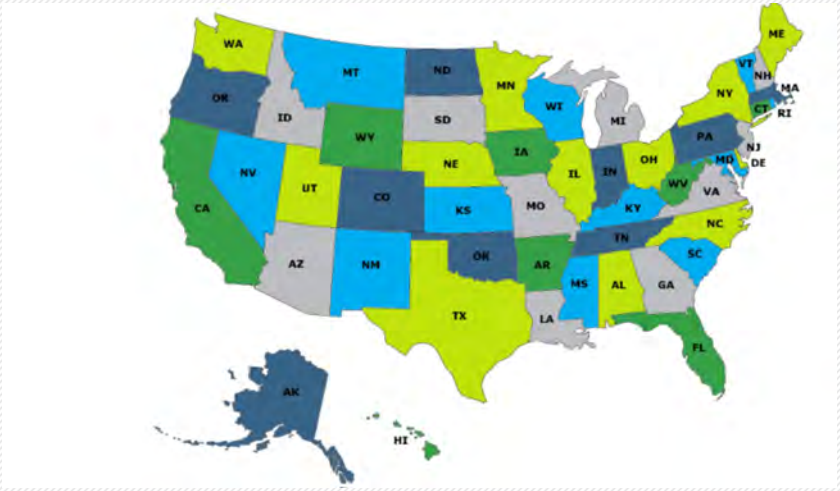
- **How Technology Plays a Role**
  - Firewalls, DNS, etc.
  - How you design your network
  - What telemetry / alerting do you have
- **How People play a Role**
  - Training and Awareness (Employees, Customers, and Vendors)
  - Testing (phishing tests, etc.)
  - Developing written policies
  - Having a way for folks to safely report potential issues.

Laws and Rules

- **Federal Laws and Rules**
  - The US has no single covering Cyber Security Law or Rule
  - It is a patchwork of various laws, depending on the agency
  - Many of the laws/rules apply to Public companies
  - A quick look: (this isn't all of them)
    - SOX (Sarbanes Oxley). Publicly traded companies
    - SEC Rule 30 (17CFR 248)
    - FTC (15 USC §45)
    - HIPPA
    - DFAR (DOD Contractors) NIST 800-171
    - COPPA (Child Online Privacy Protection Act) 15 USC §91 16 USC §312
    - ECPA (Electronic Communications Privacy Act) 18 USC §119 and 121

Laws and Rules

- **State Laws and Rules**
  - Each State has its own patchwork of laws and rules.
  - Some states have strict breach notification and reporting laws.
  - A place to look:
  - https://www.itgovernanceusa.com/data-breach-notification-laws



Laws and Rules

- **Industry Rules**
  - Various industries have certain rules or contractual requirements.
  - PCI-DSS (Payment Card Industry – Data Security Standard)
  - ISO 27001 and ISO 27002
  - NIST CSF (Cyber Security Framework)
    - NIST: identify, protect, detect, respond and recover

Why you should care?

- **Protecting your Employees**
  - You store a bunch of information about your employees.
  - Home Address, phone, bank, family members.
  - They should feel confident and safe that this information won't be abused.
  - You have policies to help protect this information from internal and external threats.

Why you should care?

- **Protecting your Customers**
  - You store a bunch of information about your Customers.
  - Home Address, phone, bank, family members.
  - Payment methods
  - Support tickets
  - Risk of exposing their internet usage information.

  - They should feel confident and safe that this information won't be abused.
  - You have policies to help protect this information from internal and external threats.

Why you should care?

- **Protecting your Business**
  - As a business you hold a ton of valuable and useful data.
  - Data that malicious actors would love to get
  - Employee data
  - Customer Data
  - Financial Data
  - Confidential Communications
  - Contracts
  - You need to have processes and policies in place to protect it

How Technology plays a role

- **Leveraging Technology**
  - The "obvious" answer is "we have a firewall". 😐
  - But is a firewall the only thing needed?
  - Do you provide DNS filtering (do you run your own recursive DNS?)
  - How are you leveraging threat feeds to help automate protection, in real time?
  - Protocols like BGP and DNS can HELP protect your network.
  - What network monitoring are you doing ?
    - Pattern of life of your network, of your towers, etc

How People play a role

- **The people are the firewall!!**
  - Proper training of your staff will go further than any firewall rule.
  - Provide awareness training for your staff AND CUSTOMERS.
  - Conduct tests (phishing tests) to help see and bring more awareness to various threats.
  - Develop written policies and processes around Cyber Security
  - When you select a new vendor, ask them how they handle cyber security. If they say they are certified, have them prove it.
  - Create a process that allows for employees, customers, public to report potential issues. THEN FOLLOW UP ON THEM

Contact Information

- **Team Cymru General Contact Info**
  - Email: outreach@cymru.com
- **Me Directly**
  - Team Cymru Email: jbrown@cymru.com
  - LinkedIn: https://www.linkedin.com/in/john-brown-cissp-020135

THANK YOU