



# CYBER SECURITY for SMBs and Startups



# Who am I?

*(...and why would anyone care?)*



- 10+ Years in Technology
- Former Army Officer
  - Signal & Cyber Ops
  - Network Warfare Leader
- Senior Tech Leader w. Multiple Global Organizations
- Network & Security Architecture, Engineering, Design
- blah, blah, blah...



**Alexander Stein**

# Who am I?

*(...why does this guy keep talking about himself?)*



Cyber Security and Full-Scope Tech Management for Small Organizations

# SECURITY IS ALL ABOUT THE FUNDAMENTALS

**AFFORDABLE**



**EFFECTIVE**

**USABLE**

A laptop screen is shown in a dark, dimly lit environment. The screen displays a line graph with a blue line and a globe. The text 'CYBER SECURITY:' is overlaid on the screen in white, underlined, with a blue dot at the end. Below it, a definition is provided in white text, with the word 'digital' in orange. At the bottom, the source '-CISCO' is written in blue, underlined. The laptop keyboard is visible at the bottom of the frame.

# CYBER SECURITY:

The practice of protecting systems, networks, and programs from **digital** attacks.

-CISCO

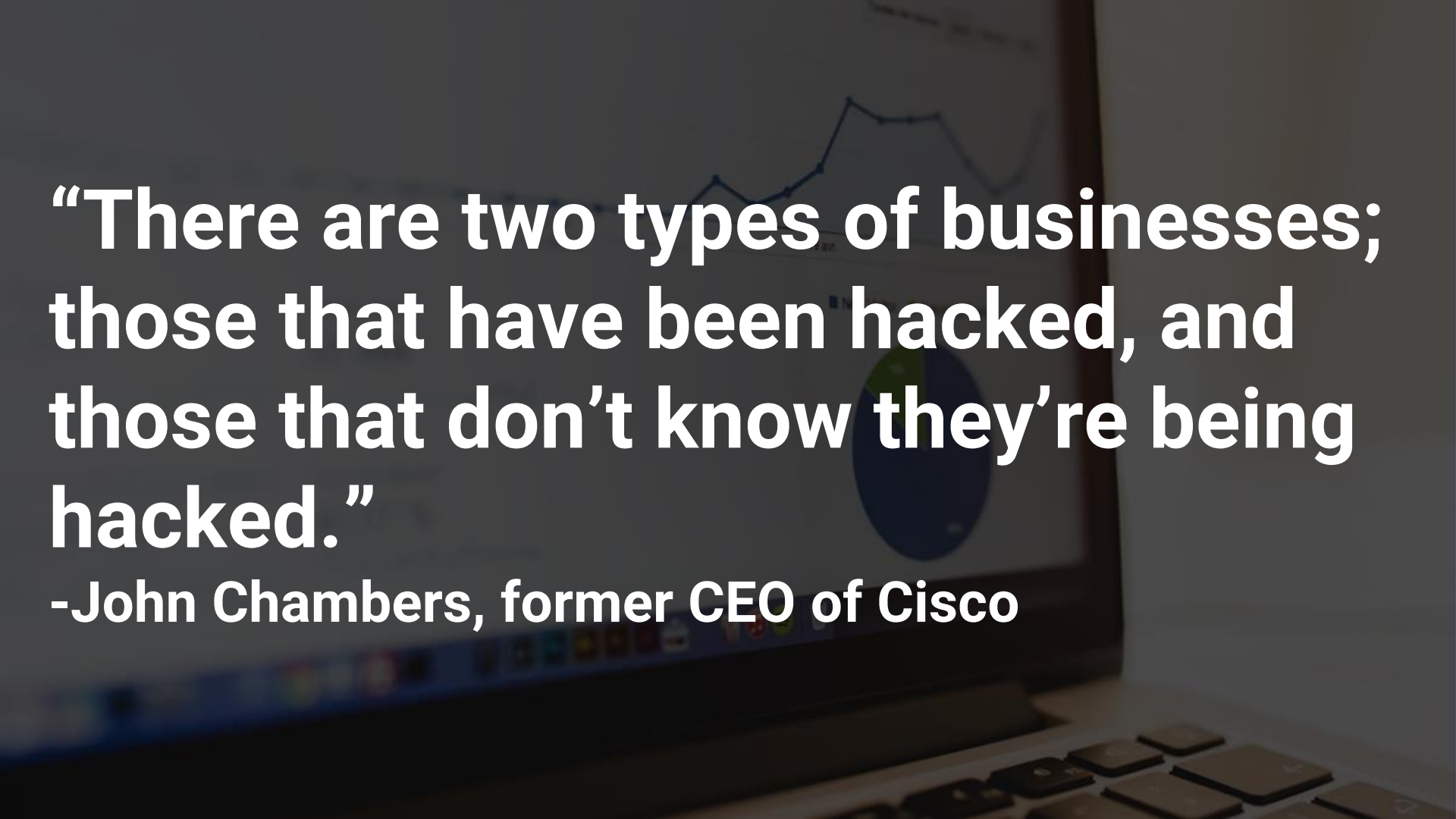


# CYBER SECURITY:

The practice of protecting ~~systems, networks, and programs~~ INFORMATION from digital attacks OR UNFORESEEN DISASTERS.

# What keeps you awake at night?



A laptop screen is shown in a dark, dimly lit environment. The screen displays a line graph with several data points connected by lines, and a globe is visible in the background. Overlaid on the screen is a quote in large, white, bold, sans-serif font. The quote reads: "There are two types of businesses; those that have been hacked, and those that don't know they're being hacked." Below the quote, the name of the speaker is also displayed in white, bold, sans-serif font.

**“There are two types of businesses;  
those that have been hacked, and  
those that don't know they're being  
hacked.”**

**-John Chambers, former CEO of Cisco**



# What is a cyber attack?

- *An attempt to steal, corrupt, destroy, or ransom digital information (or the access thereof).*
- **Hackers** often have a wide range of goals.
  - They **ARE NOT** Neo from the Matrix.
  - Most leverage pre-built, **malware-as-a-service** products to launch an attack.
- Most cyber attacks are **NOT** complex.
  - They often target already published vulnerabilities that have gone **unpatched**.
  - They exploit weaknesses in human behavior.

# Am I a potential target?

Between 2018 & 2019 approximately 50% of cybersecurity breaches involved or targeted small businesses, with a significantly increasing number of those attacks targeted against “professional services” companies like law firms, marketing agencies, and other consultancies.

[Verizon – 2019 Data Breach Investigations Report](#)

---

# Does technology pose a threat to your business?

“year over year, the worldwide spend for cyber security continues to grow...Organizations are starting to understand that malware is a publicly available commodity that makes it easy for anyone to become a cyber attacker...”

[FireEye - What is Cyber Security? Protecting your cyber assets and critical data](#)

---

# Why does information security matter?

- You collect more information than you realize.
- Cyber crime is a global industry.
- Information has **value!**
  - CC data, addresses, phone numbers, SSNs, usernames/passwords...
- Losing control of that data reflects poorly on you.
  - Can result in **criminal negligence** or **regulatory fines!**

# How can a cyber attack impact your business?

- Corruption or **loss of critical data**
- Cost of **ransoms** paid
- Damage to your IT infrastructure
- Damage to reputation
- Legal action
- **Theft** of intellectual property
- Loss of access to resources
- Legal & regulatory **fin**es for non-compliance
- Financial theft
- Increase to insurance premiums



~~\$\$\$~~


LOSS OF REVENUE

~~\$\$\$~~



# What **questions** should we ask ourselves?


1. How would a loss of technology access impact our business?
  - Can we continue to operate without it?
2. Do we have total control over all of our resources & accounts?
3. What are we doing to prevent an attack?
  - Are we **proactive** or **reactive**?
4. How would we recover from an attack or disaster?



# What **steps** can we take to answer those questions?

1. Conduct a **Business Impact Analysis** (*and BE HONEST!*)
2. Create and document two plans:
  - Cyber Security Incident Response Plan (**CSIRP**)
  - Disaster Recovery Plan (**DRP**)
3. Document your entire network
  - Include ALL computers, servers, mobile devices, software, web services, accounts, etc.
  - Don't let that documentation go stale



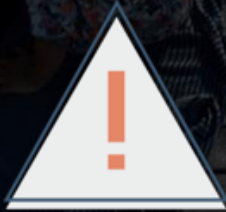


Okay great...but  
what can we do  
to **protect**  
ourselves?

1. Implement & maintain **total control** of your IT assets
2. Secure/monitor employee accounts
3. Require **2FA** at every turn!
4. Leverage strong anti-malware solutions (*not Windows Defender*)
5. **Encrypt** hard drives
6. Backup your data **DAILY**
  - Test those backups every year!
7. Patch & Update **EVERYTHING**
8. Maintain a formal standard\*
9. **Talk to a professional!!!**



Questions?





bluetec

**Alex Stein**

[alex@bluetecllc.com](mailto:alex@bluetecllc.com)

**804-852-0855**

<https://www.bluetecllc.com>

**Social:** [@bluetecllc](#)