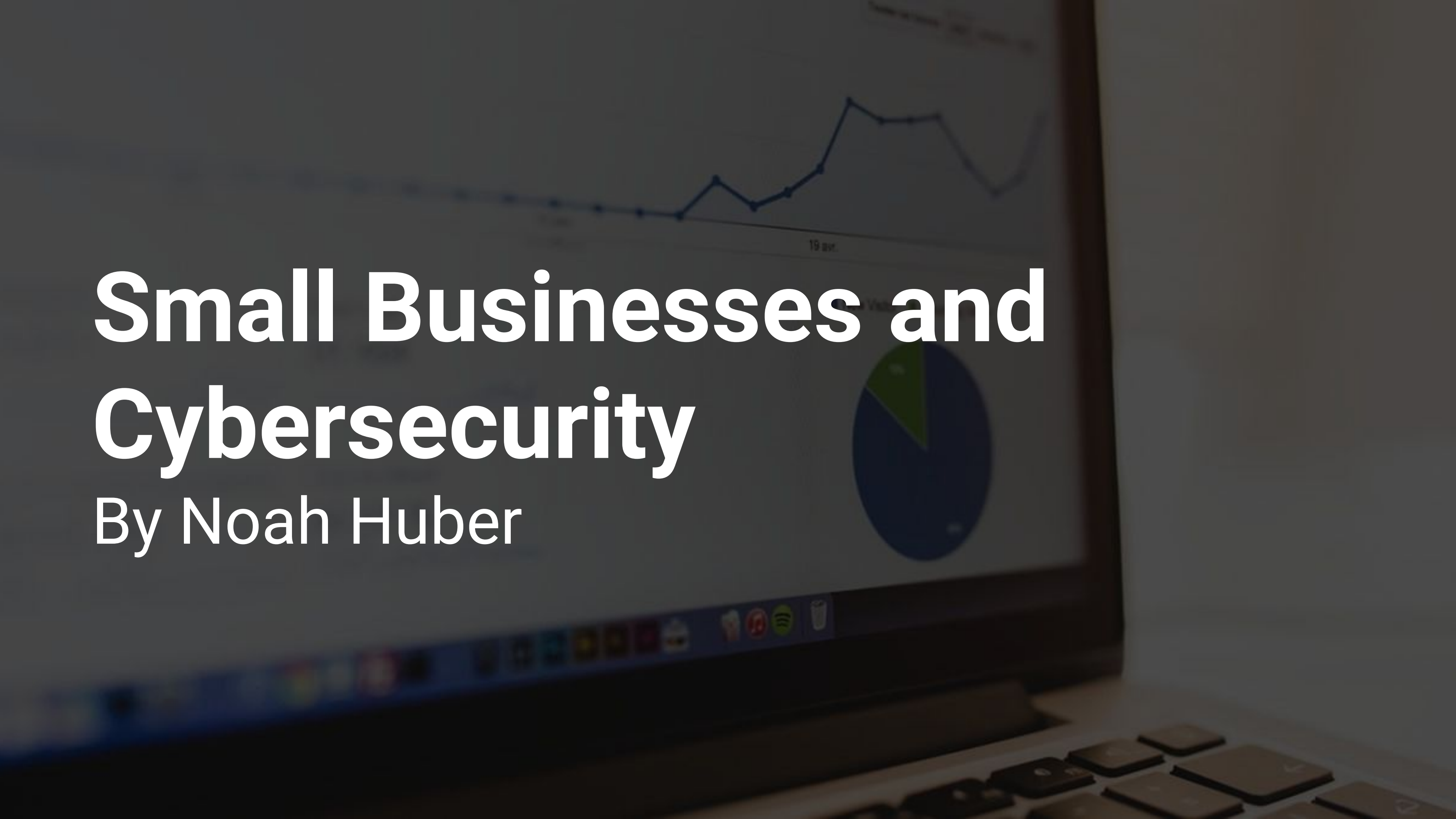


Small Businesses and Cybersecurity

By Noah Huber

Big Companies

Small Companies

Why Are Businesses Targeted?

Businesses are targets for cyber attacks due to various reasons that appeal to cyber criminals' and threat actors motivations and tactics. Main reasons to target businesses are financial gain, as businesses store valuable financial information like credit card numbers and data that can be exploited through identity theft and fraud. Extortion and sabotage are also prevalent, with attackers leveraging threats to disrupt operations or leak sensitive information unless ransom demands are met. Additionally, businesses may fall victim due to a lack of cybersecurity awareness and resources, especially among smaller businesses that lack dedicated personnel, budgetary allocations, or expertise to implement security measures.

Common Attacks

- Phishing (Email, Text, Phone)
- Ransomware
- Data Breach
- Weak Passwords (Brute-Force)
- Denial of Service Attacks
- Unpatched Software Vulnerabilities
- Vendor Vulnerabilities
- System and Operation Disruption

Cost of Cyber Attacks

Cyber attacks and exploited vulnerabilities can be costly for businesses that do not have cybersecurity measures in place. This is especially important for smaller businesses without the financial assets of a larger organization.

- Financial losses from theft, remediation costs, and ransomware attacks
- Reputational losses from data breaches.
- Operation disruptions, downtime, and corresponding financial losses.

Why Small Businesses Need Cybersecurity Personnel

Small businesses need Cybersecurity personnel for a variety of reasons.

Cybersecurity personnel help monitor, protect, defend, and respond to cyber attacks and security issues.

Incident Response Plans, Risk Management, and Training on Cyber awareness.

Communication with supervisors to inform about cyber events.

The solution

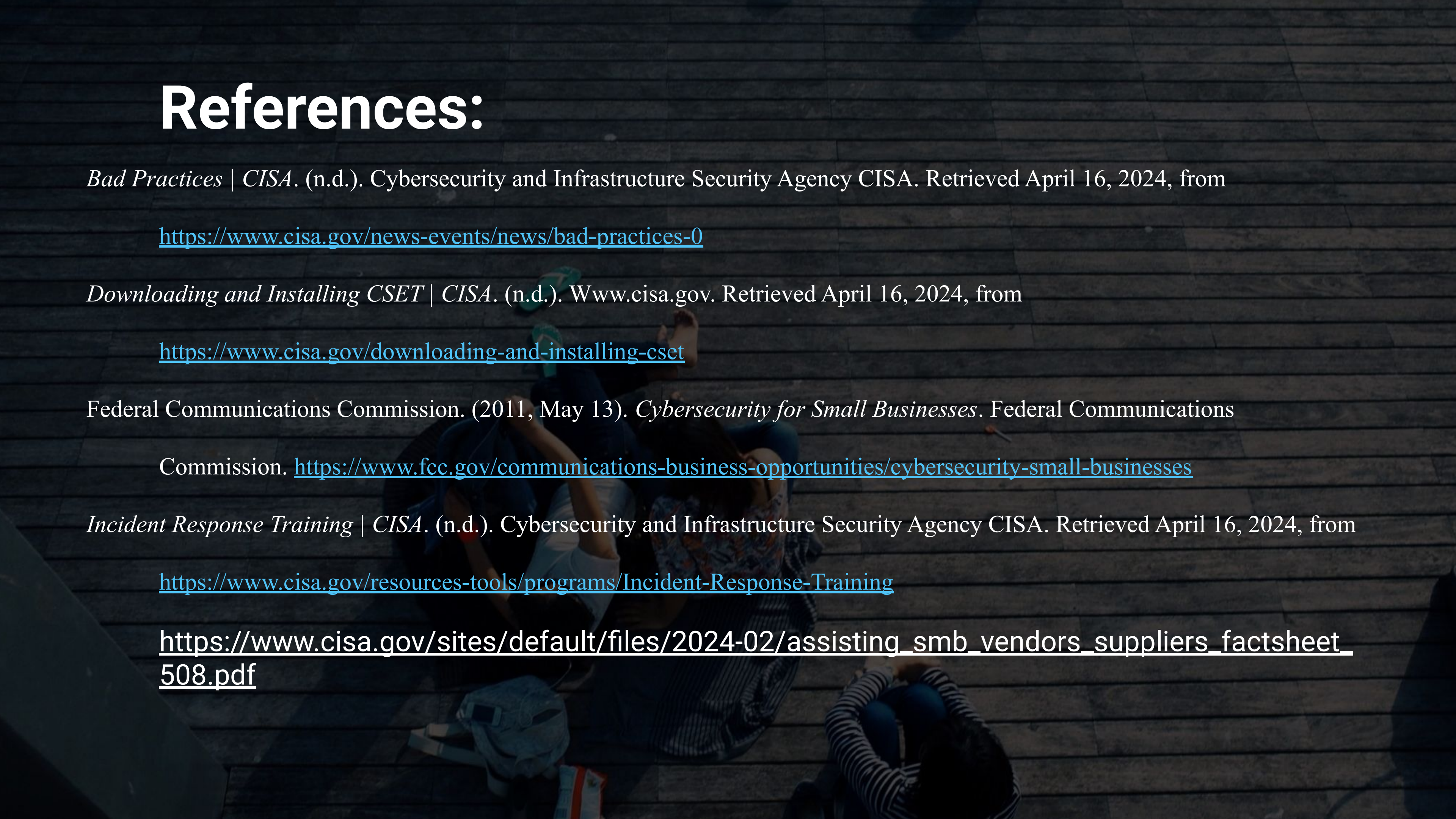
Small Businesses Should:

- Instate a Cybersecurity Analyst or a Security Program Manager as advised by CISA (Cybersecurity Infrastructure Security Agency)
- IT team cannot handle cyber threats alone.
- Ensure proper training and cyber awareness.
- Write and Maintain an Incident Response Plan (IRP)
- Vulnerability Scanning. (AV,AM)

What To Do?

If there is a major breach that occurs or a cyber threat that cannot be easily contained by the small businesses cybersecurity personnel it is important to call regional agencies that can assist. CISA has support for emergency cyber attacks. “If a significant security incident is detected while in progress, the facility should immediately call local law enforcement and emergency responders via 9-1-1.” (CISA.gov)

Have Awareness



References:

Bad Practices | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. Retrieved April 16, 2024, from https://www.cisa.gov/news-events/news/bad-practices-0

Downloading and Installing CSET | CISA. (n.d.). Www.cisa.gov. Retrieved April 16, 2024, from https://www.cisa.gov/downloading-and-installing-cset

Federal Communications Commission. (2011, May 13). *Cybersecurity for Small Businesses*. Federal Communications Commission. https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

Incident Response Training | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. Retrieved April 16, 2024, from https://www.cisa.gov/resources-tools/programs/Incident-Response-Training

https://www.cisa.gov/sites/default/files/2024-02/assisting_smb_vendors_suppliers_factsheet_508.pdf