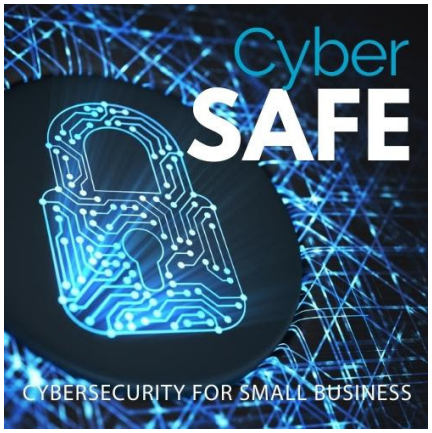
Why is Cybersecurity Essential for Local Businesses?

Why Should Local Businesses Invest in Cybersecurity?



The world is digital. Present-day business infrastructures depend on the modernization of technology—technology that provides simplicity, but simple enough to be exploited. Small businesses are most prone to cyber attacks, usually due to the deficits in their security infrastructure.

CISA *(Cybersecurity & Infrastructure Security Agency)* mentioned that "Small businesses have valuable information cyber criminals seek, such as employee and customer records, bank account information and access to the business's finances, and access to larger networks." *(CISA, 2022)* Small businesses are usually more vulnerable and are at higher risk to cyber attacks compared to larger firms. This is due to the fewer resources smaller businesses dedicate to cybersecurity, in relation to larger businesses.

It is essential that small businesses upgrade their security infrastructure to decrease the odds of a cyber-attack being successful against them.

Cyber-attacks are usually viewed as external threats, but this may not always be the case. Most cyber-related incidents actually occur within the company itself, whether it was done on purpose or an accident. *IBM* classifies these threat-actors in four different categories:

1. The Pawn
2. The Goof
3. The Collaborator
4. The Lone Wolf

1. The **Pawn** would be the innocent employee, unaware of the implications of their digital actions. Essentially, this employee could easily be duped by outside threats. If they were to receive an inauthentic email from their district manager, asking for personal identifiable information, this employee will mistakenly send this entity the information asked of them. This would compromise the businesses integrity since this outsider was able to acquire knowledge on an employee. The security issue here can escalate, but it depends on the clearance of the employee's credentials. This could then lead to company data being leaked, stolen, sold or tampered with, costing thousands, if not millions in profit losses.

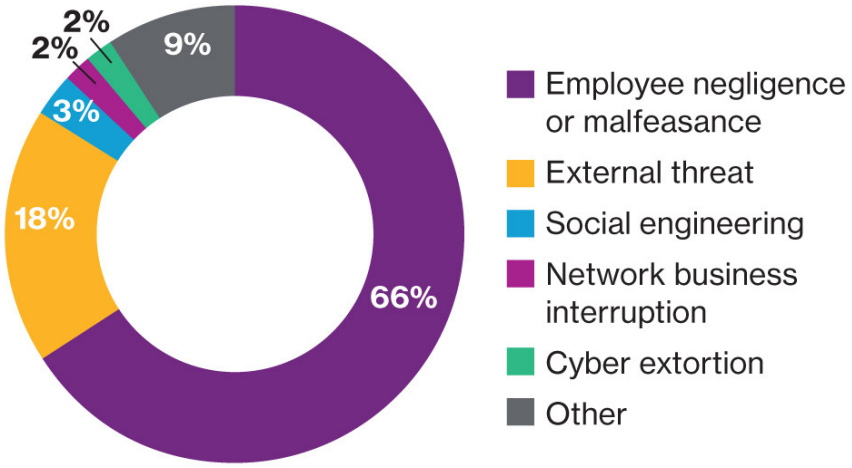
2. The **Goof** is that employee that does not properly follow company security protocols. This individual may enter restricted parts of the company, or they may take their work home, risking the exposure of business information to outsiders. In sum, the goof would make irresponsible decisions that can potentially harm the organization if not addressed accordingly.

3. The **Collaborator** is the "under-cover employee." This employee has ulterior motives, mainly which involves working with other organizations who may be competitors.

4. The **Lone Wolf** is that employee who independently works against the company. This could be for financial gain or malicious intent. The situation becomes worse if this person has an elevated privilege level where they promote leadership qualities. This can direct a business into a downward spiral.

Common Cyber Threats to the Workplace

Figure 1. **Percentage of claims by breach**



Source: Willis Towers Watson cyber insurance claims data (World Economic Forum, 2017)

How Can Local Businesses Start Preparing?

There are a variety of ways an organization can start, or safeguard, its security infrastructure. Some great approaches are:

- ➔ Employ qualified cybersecurity professionals,
- ➔ Utilize identification cards,
- ➔ Install/Upgrade security cameras that are no more than 5 years old—newer is better,
- ➔ Occasionally assess the cyber-awareness of employees,
- ➔ Update staff on any new hirees,
- ➔ Define company limitations—designate no-access/restricted zones.

In spite of this, there is always more an organization can do to improve its security capabilities. It is great to have security procedures in place, but those protocols must continuously be revised, updated and monitored to ensure a secure working environment.

There is no guarantee to circumvent a cyber-attack, but a business can increase the security of their network, making it a pain for attackers to breach and access.

Bibliography

CISA. 2022. “CISA Cybersecurity Awareness Program Small Business Resources | CISA.” https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-small-business-resources.

Federal Communications Commission. 2011. “Cybersecurity for Small Businesses.” https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses.

International Business Machines Corporation. 2022. “What Are Insider Threats? | IBM.” https://www.ibm.com/topics/insider-threats.

Subhani, Abdul. 2022. “Council Post: Generating Cybersecurity Awareness In A Business Environment.” *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2021/05/07/generating-cybersecurity-awareness-in-a-business-environment/.

UA, Little Rock. 2021. “ASBTDC Introduces Online Training to Keep Small Businesses Cyber Safe - News - UA Little Rock.” https://ualr.edu/news/2021/09/15/cyber-safe-training/.

World Economic Forum. 2017. “The Biggest Threat to a Company’s Cyber Security Is Hiding in Plain Sight.” https://www.weforum.org/agenda/2017/12/the-biggest-threat-to-your-cybersecurity-is-hiding-in-plain-sight/.

Zadelhoff, Marc van. 2016. “The Biggest Cybersecurity Threats Are Inside Your Company.” *Harvard Business Review*. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.