Entrepreneur & Innovation Exchange
Published online at EIX.org on June 10 2022
DOI: 10.32617/797-62a35ba0a30da

Protect Your Business From Cyberattacks

Joseph Simpson (Virginia Tech)

KEYWORDS: Management, Information Technology, Startups, crisis management.

The challenges entrepreneurs face seem daunting. A global pandemic, rising inflation, and a spate of other problems have entrepreneurs reeling. To add to the mix of problems entrepreneurs face, cyberattacks threaten to cripple emerging businesses. Ransomware attacks, for example, cost U.S. companies an average of $2 million per incident (Schiappa, 2022) and 88% of small business owners felt their business was vulnerable to cyber-attacks (U.S. Small Business Administration, 2021). And along with costing money, cyberattacks also undermine company reputations and their customers' and the public's confidence in them.

Taken together, this information suggests that cyber-attacks are an area of critical importance for entrepreneurs.

Entrepreneurs often avoid tackling cybersecurity because they think it's too technically complex and too expensive to protect computers. Most entrepreneurs cannot afford to hire professional IT services and systems. However, some of the most effective steps in securing your company's technology are simple and inexpensive. In this article, I provide some basic steps anyone can take that can increase their company's protection against cyber-attacks:

- Trust, but verify
- Update your systems
- Use strong passwords and multi-factor authentication
- Protect confidential information
- Seek resources and help
- Consider insurance against cyberattacks

TRUST BUT VERIFY

One of the most common methods cybercriminals use to attack companies is social engineering. Social engineering attacks occur when a cybercriminal attempts to trick someone, usually an employee, into giving confidential information (e.g., passwords, account information) over to them. The cybercriminal might pretend to be a customer service agent; they might send a threatening lawsuit in an attached PDF; or they might even pretend to be the owner of the company who needs an urgent gift card. They tend to prey on people's emotions by evoking a sense of urgency, fear, curiosity, greed, or helpfulness. Scammers often pretend to be law enforcement and will threaten unsuspecting entrepreneurs with jail time if they do not comply with their demands.

To avoid these attacks, be sure that everyone in the company understands the importance of giving information only to verified people, not clicking suspicious links or opening documents from unconfirmed sources, and when in doubt, contacting the person that sent a message or call via a trusted medium if possible. For example, if someone calls claiming to represent the IRS, you can always call the IRS back directly.

UPDATE YOUR SYSTEMS AND SCAN REGULARLY

Computers often send you update reminders. Those updates frequently help our computers to run smoother, faster, or more efficiently. However, updates are also frequently used to help secure your computer against malicious actors. Hackers often find or create vulnerabilities in systems that are not updated, and then exploit them. Neglecting to install updates leaves your system vulnerable to attack. Update early and update often!

Most modern computers ship with an anti-virus system installed on them. People often ask whether it is worthwhile to use a paid version of anti-virus or the version provided by the operating system. In most cases, free versions such as Microsoft Defender are adequate, but it depends on your business and its needs. Whether you use a paid or free version, be sure to scan your business and personal computers regularly for threats as well as to update your systems when an update is sent out. It may help to set up periodic reminders on your calendar to check if all your computers are updated and scanned.

USE STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION

Let's face it; no one likes entering a complex password into the hundred or more websites we use. Yet, we often find that the passwords we use across multiple sites are compromised. That means that a hacker might have access to multiple accounts across your company if you use the same password for all your logins or if your passwords are weak. Fortunately, entrepreneurs and their employees can use free password management software to help them create and store passwords. Sample vendors include LastPass, Bitwarden, or 1Password.

If using a password manager is not attractive, be sure to use a passphrase or, at the very least, a strong password. A passphrase is usually a combination of four words that are at least 14 characters in length. An example of a passphrase could be "The red fox ran!" Be sure not to use something that most people might know about you or include personal information that is easily identifiable. If you choose to use a password, be sure that it meets the criteria for a strong password. That means that your password should be at least 14 characters, use a combination of upper- and lower-case characters, and include numbers and special characters. Try to avoid using personal information such as your date of birth, your name, your home address, or anything else that someone might be able find via an internet search.

Finally, most software that entrepreneurs use includes the option to enable multi-factor authentication. Multi-factor authentication is simply the use of multiple methods to authenticate your login. For example, a password and a phone are commonly used multi-factor authentication methods. Entrepreneurs may worry that multi-factor authentication may slow them down in a fast-paced environment, but the cost is usually just a few seconds, and this simple measure may save you millions of dollars if your company is targeted by cybercriminals.

Protect Confidential Information

Whether the information you want to keep private is your own, an employee's, or a customer's, it is important that entrepreneurs take steps to protect it. Most mainstream email systems like Microsoft and Google allow you to encrypt messages when you send them. Be sure to use these options when dealing with confidential information. If you store information (e.g., customer bank information, patient data, etc.), ensure that only the people who need that information have access to it and encrypt the information. If possible, store information separately. For example, if the customer information includes login information, store and encrypt the account identifier and the password separately and use a common identifier to link them.

SEEK RESOURCES AND HELP

The importance of cybersecurity has become so high that many countries have government agencies that provide free resources and assistance to companies. For example, the United States' Cybersecurity & Infrastructure Security Agency (CISA) and Federal Trade Commission (FTC) provide comprehensive resources for small businesses and entrepreneurs. Most of the solutions they provide are free and easy to implement. Many other free resources are available. Sometimes, however, cybersecurity solutions need to be tailored to a company and outside help should be enlisted.

Consider Cybersecurity Insurance

All entrepreneurs should give cybersecurity insurance some thought, especially if they store any type of sensitive customer information (e.g., credit cards, medical information). The costs for such insurance ranges from around $500 to over $5,000 annually. Cybersecurity insurance is more of a necessity for some industries and less so in others. For example, a restaurant that doesn't store customer or other sensitive information would be unlikely to need cybersecurity insurance, but a payment systems firm would likely need it.

In Case of a Breach

Upon discovery of a data breach, immediately seek to contain the issue and fix the vulnerability if at all possible. In many cases, this means removing the affected device(s) from online connectivity. Depending on the state and industry, businesses may be required by law to report the incident. Check your respective laws for these requirements. Consider contacting a lawyer for advice. Notify local police and all affected parties. Investigate the source of the breach and change

DOI:
10.32617/797-62a35ba0a30da

security policies and procedures accordingly. And this may be the time to bite the bullet and hire a professional to get you back on track.

CONCLUSION

Cybersecurity is often scary because it seems beyond the technical capability of most entrepreneurs. However, some of the most effective solutions for cybersecurity and preventing cyber-attacks are free and simple to use. These suggestions are easy to implement for your business as well as for your family's computers.

REFERENCES

Schiappa, D. (2021). With Ransomware Costs on the Rise, Organizations Must be More Proactive. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/07/13/with-ransomware-costs-on-the-rise-organizations-must-be-more-proactive/?sh=27d093252dd5.

U.S. Small Business Administration. (2022). Stay Safe from Cybersecurity Threats. Retrieved from https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats.

EIX.org (2022)
DOI:
10.32617/797-62a35ba0a30da