TITAN TIMES NEWSLETTER

January, 2021

TITAN BUSINESS DEVELOPMENT GROUP, LLC

A Primer on Cyber Threats

The damage related to cybercrime is projected to hit $6 trillion annually by 2021, according to Cybersecurity Ventures. A few billion of that will be borne by small businesses alone. Small businesses are attractive targets because they have information that cybercriminals want, and they typically lack the security infrastructure of larger businesses.

According to a recent SBA survey, 88% of small business owners felt their businesses were vulnerable to cyber-attacks. Yet many businesses simply cannot afford professional IT solutions, have limited time to devote to cybersecurity, or they do not know where to begin. Cyber-attacks are constantly evolving, and business owners should at least be aware of the most common types so they can take some preemptive actions.

Malware

Malware (malicious software) is an umbrella term that refers to software intentionally designed to cause damage to a computer, server, client, or computer network. Malware can include viruses and ransomware.

Viruses

Viruses are harmful programs intended to spread from computer to computer (and other connected devices). Viruses are intended to give cybercriminals access to your system.

Ransomware

Ransomware is a specific type of malware that infects and restricts access to a computer until a ransom is paid. Ransomware is usually delivered through phishing emails and exploits unpatched vulnerabilities in software.

(continued)

Inside this issue:

TITAN
Business Development Group, LLC
coaching | consulting | results

Phishing

Phishing is a type of cyber-attack that uses email or a malicious website to infect your machine with malware or collect your sensitive information. Phishing emails appear as though they have been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, your computer may become infected with malware.

Here are a few basic cybersecurity best practices:

> *" Phishing is a type of cyber-attack that uses email or a malicious website to infect your machine with malware or collect your sensitive information."*

Be vigilant when it comes to emails

Be careful about clicking on links or opening attachments in emails that come from sources you do not know or trust. Nowadays, many malicious emails are sent out that look legitimate but can be identified as bogus by looking at the sender's email address.

Train your staff

Employees are a leading cause of data breaches for small businesses because they are a direct path into your systems. Training employees on basic internet best practices can go a long way in preventing cyber-attacks. Make them aware of actions such as: spotting phishing emails, using good browsing practices, avoiding suspicious downloads, creating strong passwords, and protecting sensitive customer and vendor information.

Use antivirus software and keep it updated

Make sure your business's computers have antivirus and antispyware software installed and that they are updated regularly. Most software can be easily set to install updates automatically. Importantly, this in NOT an area to try to scrimp and save money on.

Secure your networks

Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

Use strong passwords

Strong passwords may include:

- 10 characters or more
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

(continued)

Consider using Multifactor Authentication

Multifactor authentication requires additional information to log in, such as a security code sent to your phone. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account(s).

Back up your data regularly

Regularly back up critical data such as word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically if possible - daily is great, but at least weekly, and store the copies either offsite or on the cloud.

Control physical access

Laptops and tablets can be particularly easy targets for theft or can be lost, so lock them up when unattended and be sure to create a separate user accounts if more than one person has permission to use the laptop.

***

Masterful Quotes

"There is one thing stronger than all the armies in the world, and that is an idea whose time has come."

- Victor Hugo

"The great thing in the world is not so much where we stand, as in what direction we are moving."

- Oliver Wendell Holmes

Eight Tips For a Stronger Business

- ✓ *Complacency is a threat.* Take a good, long look at your business. Do you see neglected areas? Complacency can be infectious. If you have stopped paying attention to the small details, your employees will do the same. If you aren't consistently and intentionally moving forward, your business may stall.

- ✓ *Find your niche*. Trying to sell to the right client is much more important than trying to sell to everyone. The more you try to please everyone, the more watered-down your offering becomes.

- ✓ *Don't confuse motion with progress.* You should be doing something every day to move your business forward. Don't confuse this with simply keeping busy.

- ✓ *Treat your business as you would your child.* As parents, we often put the needs of our children in front of our own. Many tend to do the opposite with their businesses, taking from them because of a sense of entitlement. You should be very careful to nurture and protect your business and carefully weigh its needs in line with your own.

- ✓ *Always have an objective.* If you make a habit of always asking yourself what the objective of each of your activities is, you will quickly find that you will begin eliminating activities that don't really benefit your business.

- ✓ *Embrace fear.* Fear protects, clarifies, adrenalizes, and usually forces us to consider things more completely. Embrace fear rather than running in response to it.

- ✓ *Stand firm on your Accounts Receivable policy.* You may feel compelled to extend overly-generous terms to friends and long-standing customers, but don't confuse having good intentions with the needs of your company. It needs a healthy cash flow the same as you need oxygen and it is your responsibility to make sure this flow remains as steady as possible.

- ✓ *Don't sell a product or service; sell a solution.* Determine what the exact solution your product or service provides, is, and sell that solution first and foremost.

***