TECH BYTES

NOVEMBER 2021

People don't usually think about small businesses when discussing cyber security. The media covers breaches in governmental and big-business security because it is "newsworthy". These entities usually have lucrative targets that attract the attention of hackers but are often backed up with an extremely protective network security system that's difficult to crack. When hackers can't break the big system, they turn their attention to easier targets.

While most hackers want the opportunity to crack a high-risk target, these situations are few and far between. Instead, they turn their attention toward much lower-hanging fruit. This is where small businesses come in; they still have access to money and data but have much lower defenses than a governmental entity. Luckily, many average cyber security strategies can keep the would-be hackers away.

Hackers methods are always changing, and it helps to be one step ahead of the game.

Cloud Security
As more and more businesses switch from hard-drive data storage to remote databases, Cloud Security is becoming more and more commonplace. Methods of providing cloud security include firewalls, penetration testing and virtual private networks (VPN), to name a few.

While many people feel that their data and information are better stored on a hard drive on their own network, data stored in the cloud may actually be more secure, depending on the system's defense strategy. Be wary, though: not all cloud security is made the same. Do your research and pick one that will best protect your data.

Continued on pg.2

Fraud Awareness WEEK

Nov 14-20th

This month is a prime time to implement new habits or ramp up current practices to prevent online scams and avoid fraud. The FBI reports that cyber crime losses topped over $4.2 billion in 2020 alone; don't let criminals take what you have worked so hard for. Take these steps:

- Set strong online passwords; do not use the same password for every account and every website
- Keep personal information personal; hackers use social media to determine your passwords
- Watch out for phishing scams; fraudulent emails & websites
- Keep your software, computers & mobile devices up to date
- Business owners: Be sure to use a dedicated workstation to perform all company banking activity
- Make sure the websites your employees buy from use secure technology & practices
- Do not allow your company devices to connect to public wifi networks

Cyber RESILIENCE

- What do you need to know?
- How can you be protected?
- How much money can you lose?
- Ask us today!

BLUE BAY TECHNOLOGY

Continued from pg. 1

Network Security
Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse or theft. This is what your network administrator will need to put into place in order to keep your devices and data secure. The best approach to protecting your network is to create a strong network and WiFi passwords, restrict downloads/website access and use system administrator accounts to enable exceptions. Passwords using random numbers and letters work best for a small business since nobody but those who need it will be able to guess the password.

VPNs And Firewalls
A VPN can help protect your security by masking your IP address. This essentially means that you'll be connected through a different server, making it much harder for the cyber criminals to pinpoint your location. A firewall is simply a shield that protects your computer from the Internet. Firewalls can help restrict access to sites that could be damaging to your network. Both of these tools can be highly effective when used properly, but they do not protect against all threats.

Updates And Upgrades
While it might seem simple, consistently updating and upgrading your technology tools can keep you much more secure. The developers of many of these tools are constantly looking for new threats that pose a risk to their program. They'll issue patches to make sure any holes are filled. You just need to make sure that all of your tools are updated in a timely manner and verify that the updates are installing.

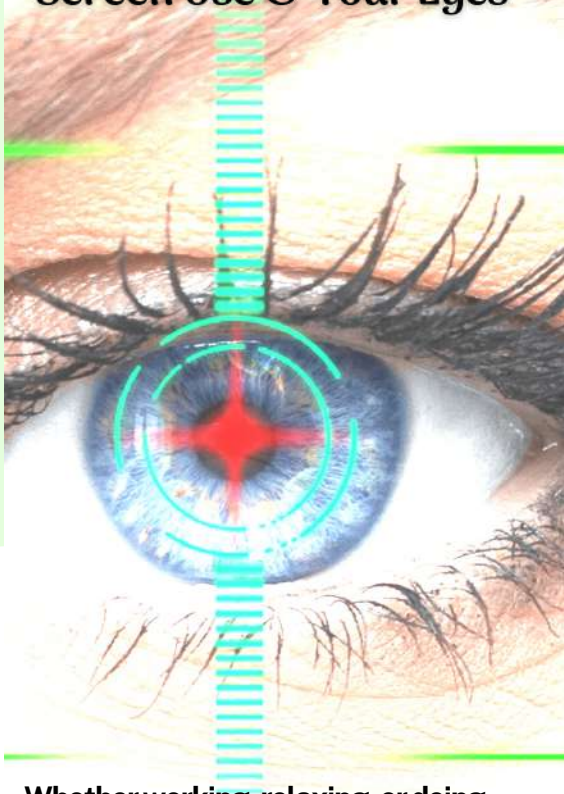
Data Backups
Always have multiple backups of your business's data. You never know when a power surge or a natural disaster might cause your current files to be deleted. You can prevent this issue by regularly backing up your data using local and Cloud backup options.

Employee Training
It's important to limit employee access to systems and company data. Not everyone needs to have access, so only give it to those who can't work without it. There should also be some type of security training for all employees. Phishing schemes and weak passwords create just as many issues as hackers.

Finally, you should make sure everyone in your workplace is security-conscious. A single breach could critically hurt your business. Your employees need to understand this so they can be proactive: If you "See something, Say something."

No matter which route you take, the most important thing you can do for your small business is protect its network. Governmental entities and big businesses do not suffer from security lapses nearly as bad as small businesses. A security lapse can stop your business dead in its tracks.

DIGITAL
Screen Use & Your Eyes



Whether working, relaxing, or doing your financial banking on your phone -- you use screens A LOT. By the end of the day your eyes may be dry and your vision may be suffering. Blurry a bit?

Normally we blink 15-20 times a minute, but people blink half as often when viewing a screen - which causes dryness. A few changes to device use can be easier on your eyes:

- **Wear contacts? Give your eyes a break & wear your glasses some**
- **Every 20 minutes look away from the screen and look at an object that is 20 feet away from you**
- **Make the text on your screens larger & adjust brightness**
- **Use artificial tears to refresh your eyes when they are feeling dry**
- **Take breaks of at least 15 minutes at every 2 hour screen time interval**
- **Raise the refresh rate on your device for less screen flickering**
- **Get regular eye exams to ensure your optical health is optimized**
- **Lower the color temperature of your screen to reduce blue light**
- **Consider a glare screen for your computer monitor**

-from WebMD

Hiring THE BEST STAFF

Not long ago, I had the opportunity to sit down with Carter Cast, the author behind **The Right & Wrong Stuff: How Brilliant Careers Are Made And Unmade**. Hiring success has a great influence on career success, and we discussed five negative archetypes that confront employers while filling a job opening. Together, we discovered some telltale signs that your interviewee may fall into one of these categories.

Captain Fantastic: While it might seem like "Captain Fantastic" would be a vital part of your team, they often cause division. Someone who is a "Captain Fantastic" is usually overambitious and has no qualms about stepping on others to get ahead. If you're interviewing a candidate and they mention that their greatest accomplishments revolve around beating others rather than delivering value or developing teams, you probably have a "Captain Fantastic" on your hands.

Solo Flier: Have you ever worked with someone who thinks their way is the best and only way to do something? It's very frustrating. While this type works well individually, they can be detrimental to a team environment. They usually claim to have no time or were too busy to accomplish their tasks; in reality, they may fail to hire and delegate properly. I've met with many people who fit this category and end up leaving their job due to burnout after taking on too much work.

Version 1.0: Change is a necessity in the workplace, but sometimes, people prefer to stick to their routine. To spot these people in interviews, listen to their stories and pay attention if they mention changes in the workplace and how they responded. If they stayed on the same path, that's a red flag. I knew a manufacturing executive who failed to adapt to new technologies. This caused him to lose some of his biggest clients, and the business fell into a tailspin.

The One-Trick Pony: These people usually get stuck in a rut because they rely on their greatest strength to solve all problems. They will often aim for lateral moves rather than trying to broaden their horizons. I interviewed a one-trick pony recently who wrote amazing copy but struggled when meeting with clients face-to-face. His communication skills weren't strong enough to work with clients or lead large teams. His career became stagnant even though he was eager to grow and move up.

Whirling Dervish: Energetic employees improve morale and production in a workplace, but sometimes lack the follow-through needed to complete projects. You can usually spot these people in interviews if you notice them avoiding your questions. They often come up with excuses for why they didn't achieve results. Great ideas and strong morale do not make up for a lack of completion.

With knowledge of these archetypes, you can avoid hiring the wrong candidate for your team and instead focus on finding the **PERFECT** fit.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best-sellers. He stays active in his community and has advised many government officials.

Storytelling is More Important
THAN BUILDING A PRESENCE ONLINE

Social media has become an ever-important tool in the business world. It can help build customer loyalty while also being an essential marketing strategy. However, simply having an account is not enough.

In order to grow, you need to understand your customers and what motivates them. Provide them with an experience they won't be able to obtain anywhere else. Be sure to do this while also making your social media content relevant. If your account does not focus on your products or services, it will prove useless. Build connections with and focus on your customers. Without trying to approach a specific type of customer, your message can get lost. It can be difficult to attract all of your customers at once.

More important than the rest is to make your presence authentic and accessible. Keep the big picture in mind and don't get lost in the weeds.

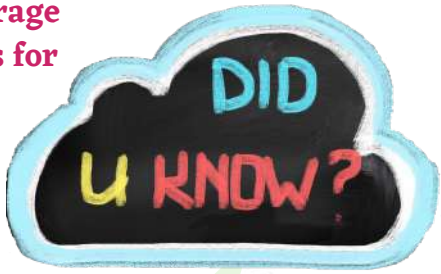
On average, people have 2 to 8 networked gadgets.

More than 500 hours of video are uploaded to YouTube every minute.

123456 is the most common password in the world.

The QWERTY keyboard was designed to slow down the typing speed.

$200,000 is the average cost of cyber attacks for companies.



32% of Internet users are 25 to 34 years old.

Until 2010, carrier pigeons were faster than the internet.

60% of small & midsize businesses fold within 6 months of a cyber attack.

90% of emails contain some form of malware!

People read about 10% slower from a screen than from paper.

Cybercrime cost $3.5 billion for US businesses in 2019.

Hackers attack every 39 seconds.

BLUE BAY TECHNOLOGY

This monthly publication provided courtesy of Will Sperow, CEO of Blue Bay Technology.

OUR MISSION: To provide our clients with the same expert-level of support that we would expect ourselves; provide it in an understanding and compassionate environment; and, work to exceed your expectations.

600 Airport Road Winchester VA 22602
4451 Brookfield Corp. Dr, Ste. 100, Chantilly VA 20151

703 261-7200

www.bluebaytechnology.com

BLUE BAY TECHNOLOGY