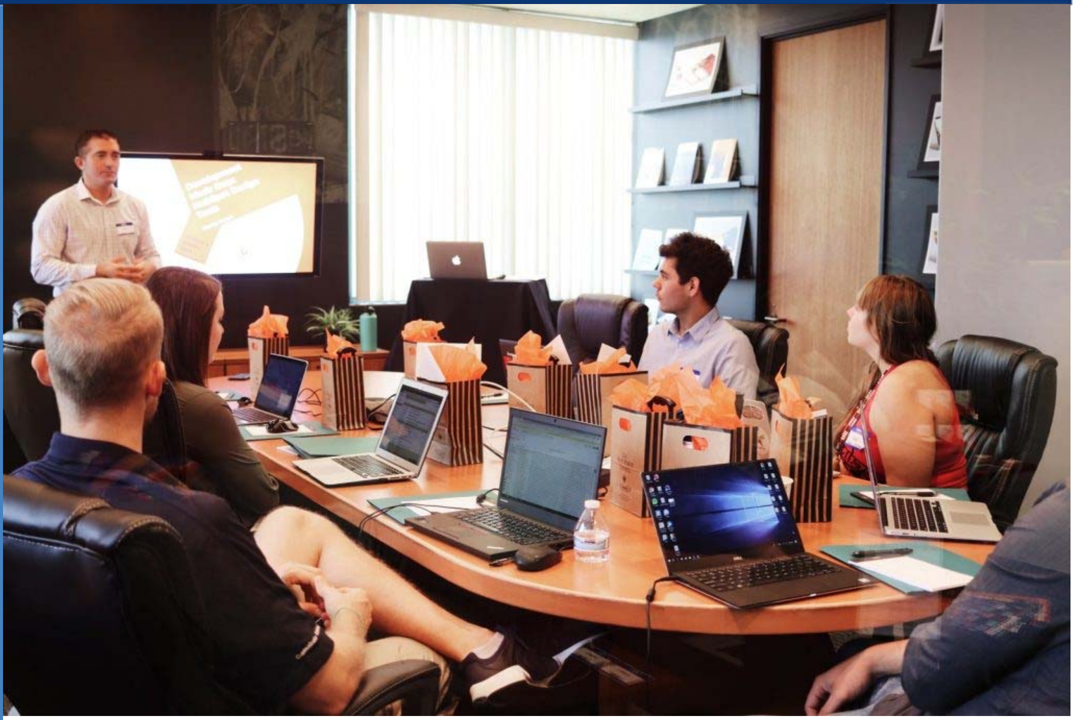
DTS DanTech Services
Computers under control!™

Technology Times March 2020 Issue

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

What's Inside:

Got IT Problem? - Click Here!



How to Protect Your Small Business From a Cyberattack

By Joe Galvin, Chief Research Officer at Vistage

Like a heart attack, a cyberattack can strike at any moment — and cause almost instantaneous damage to your company's productivity, credibility, financial security, and more. Beyond the trouble, this threat is expensive. According to the National Center for the Middle Market (NCMM) at The Ohio State University Fisher College of Business, hackers cost the global economy a staggering $350 billion each year.

As Chief Research Officer at Vistage, I know that the majority of cyberattacks happen to small and midsize businesses (SMBs). Hackers call these companies "soft targets" because they often lack sufficient security measures and personnel to thwart an attack. Some SMBs don't back up their files offsite, which makes them vulnerable to ransomware and many have data that can be leveraged to break into larger companies.

The problem is, most SMBs are not fully prepared to defend themselves against a cyberattack. According to a Q4 2018 Vistage survey, 57% of SMBs don't have an up-to-date or active cybersecurity strategy. Of the 1,257 CEOs who participated in the survey, only 43% said their company had a cybersecurity strategy in place that was both current and reviewed on a regular basis.

If you fall into that majority, it's time to mitigate the risk. Start with these three areas for a layered defense and strong cybersecurity strategy for your business.

- Continued on page 3

AAAP

That's an acronym:

Another Article About Passwords

It gets as old reading about them as it does to write about them, yet passwords are your front line of defense when it comes to protecting your data. Passwords, along with factored authentication, protect you. Factored authentication might be MFA (Multi), 2FA (Two), or a smart card, USB dongle, finger-print, or other biometric recognition—like FaceID on an Apple iPhone.

For once, I'm happy to report that NIST (National Institute of Standards and Technology) has new recommendations that reduce the complexity and time requirements of passwords while strengthening them by a significant degree of complexity by using "passphrases."

Here are the recommendations from NIST for your organization:

- Require everyone to use longer passwords or passphrases of 15 or more characters without requiring uppercase, lowercase, or special characters.
- Only require password changes when there's a reason to believe your network has been compromised.
- Have your network administrators screen everyone's passwords against lists of dictionary words and passwords known to have been exposed on the Dark Web.
- To help prevent a denial of service attack against your email service, don't lock a user's account after a certain number of incorrect login attempts.
- Don't allow password "hints."

While this won't change how software providers and web portals, such as banks, set their requirements, it can have a drastic effect on computer login passwords that are managed by your administrators.

Two key ingredients:
- no more "every X day" password changes;
- use of a passphrase of 15 characters or more;

The reason for the longer length has to do with the function of computing power and time. To see this in action, go to https://randomize.com/how-long-to-hack-pass/ and put in a short, 8 to 10 character password and a longer, 15, or more character passphrase.

These changes to security will make life easier for many of us that have struggled with the complexity of requirements that can create more havoc & chaos while at the same time, keep us from doing our jobs.
There's even a site for this at https://randompassphrasegenerator.com/ that helps to put random words together. **Tip**: generate a few different phrases and select what works best for you.

Disasters: Natural, Man-made, and COVID-19

Alaska is no stranger to catastrophic events. We only need to reflect on November 30, 2018, and the 7.1 earthquake that hit our South Central region. Or consider all of the state fires in summer 2019, the floods, and record snowfall. Any single event could disrupt our lives fast and unexpected. The need to consider and plan for how we respond to emergencies became even more apparent than any warning message, because we 'lived' it.

The risk management profession has a mantra: avoid, accept, reduce/control, or transfer. Those are the choices we have when a crisis emerges. Now, we face a global crisis: the Coronavirus (COVID-19) has affected industries, travel, financial markets, and countries, and maybe even someone you know.

According to the CDC, it's not a matter of if, but when we see the more substantial effects of this deadly disease hit the United States. To what extent we don't—and won't—know until we can look back on this potentially disastrous problem. What matters is how we prepare for and respond to what can and might happen to unwanted but identifiable risk. **Avoid, accept, control, or transfer?**

Have you considered how this could affect your business?

Can your business transition to a decentralized, remote-worker, or skeleton staffed operation?

Prior considerations and planning should happen now—well before it becomes a necessity. With planning, your business will be able to mitigate the chances of the next crisis crippling your ability to stay in business.

DanTech Services is here to keep your business going. We shift risk away from your company when disaster happens – what engineers and risk managers can "transfer" of risk through decentralization. We are experts in working remotely and in a decentralized manner.

We've also got the experience needed to support our clients should they need to provide employees access to their desktop resources at their regular office while working from home.

We did this for one of our clients after the 7.1 2018 earthquake: we physically moved their workstations and servers to another facility, and then provided the staff with access to their workstations so they could access their server resources.

Were there challenges and problems to sort out? Of course. Yet none of them were insurmountable. More important, they were able to continue to work, to service their clients, and to meet their payroll. They were able to keep their doors open – literally and virtually.

Ready to Transform Your Business With Technology?

Technology, the change agent of our generation, is transforming the business landscape by enabling small and midsize businesses to streamline processes, improve productivity and get ahead of competitors.

Despite this, only half (51 percent) of CEOs have a digital business strategy underway. Why is this a problem? Without a well-defined strategy, CEOs end up learning lessons about digital transformation the hard way. This is especially true when it comes to technology integration, which many CEOs are ill-equipped to handle; only 37 percent of respondents said they have dedicated IT staff.

Spare yourself the pain. Follow these five technology truths shared in our latest report.

1. Get used to this pace. Technological advancements won't ever slow down. They'll just continue to get faster. Blockchain, artificial intelligence and 5G networks are already here, ushering in the next seismic wave of change. The reality is, you'll always be under pressure to keep up with the next best thing -- but a clear strategy will help you know where to direct your investments.

2. Expect to spend. It's not a good idea to short-change investments on infrastructure, applications and IT talent that are critical to your business. Technology isn't cheap and will usually cost more than you think. Accept the fact that quality comes with a cost, and the alternative is automating chaos.

3. Realize that transformation is hard. IT projects will always take longer, cost more and be more difficult to complete than you originally thought. The combination of shifting to digital-first thinking and transforming ingrained processes will test you, your team and your employees in ways you never considered.

4. Tighten up your cybersecurity. The benefits of using data to manage your customers, employees, operations and financials carry significant risk in the form of cyber threats. Every day, cybercriminals are working to exploit vulnerabilities in your digital security, and they'll never let up. If you have digital IP, your business is all about your data, so you need to protect it as vigilantly as your cash and investments.

5. Remember that it's still about people. Technology can do amazing things. But it's only powerful when it empowers leaders, managers and workers to make better decisions, and when it provides information that improves productivity. It's how customers use technology to engage with you -- and how your people use technology to get closer to your customers -- that propels a digital-first company into the future.

"How to Protect Your Small Business From a Cyberattack"
- Continued from page 1

1. Bring awareness and training to employees

Train your employees to abide by basic security principles, such as using strong passwords, maintaining appropriate internet use, and handling customer information and data with care. Teach them how to spot an attack by using internal phishing simulations. Communicate why this training is important and what's at stake for the company by making it personal.

Why is training so important? Because 90% of breaches, whether in the form of ransomware, BEC or another type of cyberattack, are caused by employees that fell for a phishing attempt, notes Cynthia James, CEO and principal consultant at Cyberus Security.

"Training users not to fall for phishing is really, really important," James says. "Once people learn the things they need to do better, they will do them eagerly."

Our Vistage survey showed that 67% of SMBs work with an external partner to manage their cybersecurity. If you're on a budget, hire a fractional CIO (contract or third-party service provider) to get IT experts when you need them. Or maybe you can build a team of unofficial deputy IT managers who shadow IT personnel to create more redundancy in security by spreading out responsibility.

2. Implement robust policies, processes, and procedures

Develop an acceptable use policy concerning how employees are allowed to use technology assets, from hardware to software programs. Provide guidelines for social media use as well. Limit employee access to sensitive data and information by tailoring their access to fit individual roles. Create a playbook for different cyberattack scenarios and work through them like fire drills each quarter.

Put someone in charge of checking firewall and anti-malware logs. Meet with a cybersecurity expert on a biannual basis and conduct an external review of IT to ensure the data and network of your organization are secure. Set up an RSS feed to tune in to the latest cybersecurity news.

3. Make smart technology choices

Invest in technology solutions like antivirus software, which defends against most types of malware. Or investigate endpoint security solutions, which cost about the same as anti-virus software and can be more effective in practice. Put firewalls in place to prevent an unauthorized user from accessing a computer or network.

Back up data so you can recover information lost in an attack. Use encryption software to protect sensitive data, such as employee records, client and customer information, and financial statements. Incorporate two-step authentication or password-security software to reduce password cracking. When sourcing technology, be sure to choose service providers with strong security.

Takeaway

Creating a layered defense that supports your people, process and technology is the best way to protect your business.

For more insights for how to protect your small to medium-sized business, visit our website: **#ProtectTheClick**

Shiny New Gadget Of The Month:

HYDROFOILER XE-1

Spoiler Alert! It’s expensive!

Using the same technology as America’s Cup sailboats this Hydrofoil eBike opens up a whole new cycling frontier. Suitable for a wide range of fitness levels, riders can explore ocean coastlines, train along waterways, or cruise lakeside with friends and family.

Fast and maneuverable, get ready to experience the thrill of cycling on the open water - no roads, no traffic.

- Variable pedal assist can be dialed up or down to fit your needs.
- Top speed of up to 12 mph (similar to traditional sailboats).
- Modular design for quick assembly and transport to and from the water.

In order to guarantee a dynamic ride experience, Manta5 was producing a limited production run that was delivered to New Zealand customers for their 2019 Summer. Very shortly after, international production and assembly began.

Although production will scale, a focus on quality dictates the size of production. From April 2020 onward, Manta5 will only be producing and shipping limited production runs globally each month.

Delivery is done on a first-in, first-served basis according to the date of your reservation. If you dream of foiling in Summer 2020, reserve now.

$7,490.00 USD

“Disasters: Natural, Man-made, and COVID-19”
- Continued from page 4

Let’s hope that all we’re discussing is possibilities and planning; that we never have to actualize those plans. But identifying potential problems and responses is the stuff of risk management. We’re here to help your organization plan a response for what could be inevitable. Let’s start that conversation. We can work to outline a plan to handle your technology and access to its resources using remote connectivity methods you’ve seen us use when we work on your computer.

Are there challenges? Yes.

- Too many users attempting to connect into a network could overwhelm the capabilities of their Internet access.
- Re-directing print jobs may not always be a suitable or workable action.
- Additional training may need to happen to bring staff up to speed.
- Your business may have special requirements or needs that don’t fit well into a drastic shift in operations or logistics.

Are there benefits? Yes.

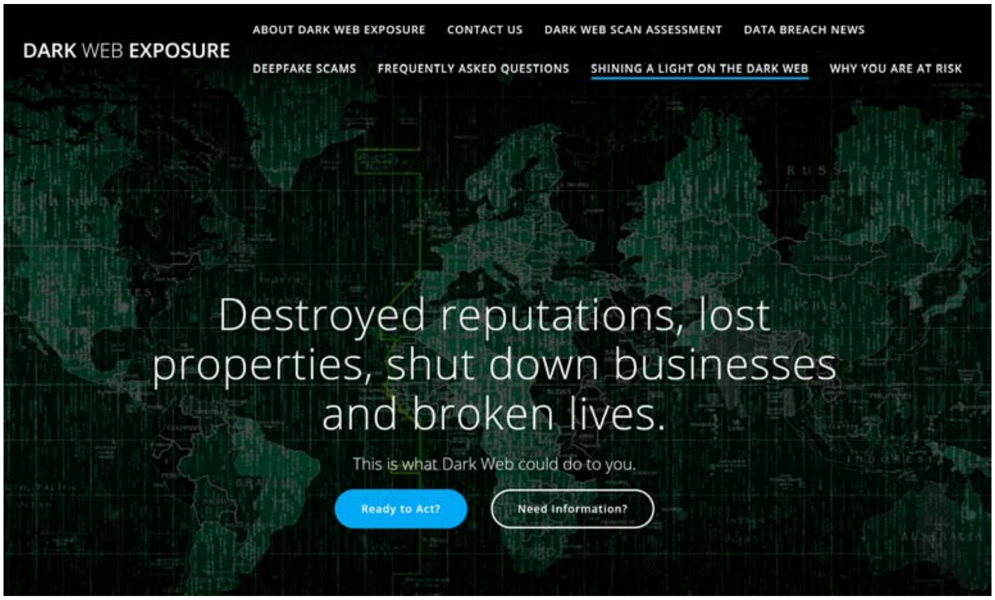
The primary benefit might be that your business survives.

Please call or email us if you have any questions at 907-885-0500 or info@dantechservices.com

NOT SURE IF YOUR ONLINE ID IS COMPROMISED?

Dark Web ID leverages a combination of human and artificial intelligence that scours botnets, criminal chat rooms, blogs, Websites and bulletin boards, Peer to Peer networks, forums, private networks, and other black-market sites 24/7, 365 days a year to identify stolen credentials and other personally identifiable information (PII).

GO TO HTTPS://DARKWEBEXPOSURE.COM TO GET YOUR REPORT!



Destroyed reputations, lost properties, shut down businesses and broken lives.

This is what Dark Web could do to you.