BACS CONSULTING GROUP

3 Steps You Can Take Today to PROTECT YOUR BUSINESS FROM UP TO 90% OF ALL CYBER ATTACKS

There's a misconception out there that has to do with the fact that, while cyber attacks are becoming more common all the time, it's really only the large, national or multi-national corporations that have anything to worry about. You'd be forgiven for assuming this is true, because it does make a certain degree of sense.

You'd be forgiven, but you'd be wrong.

According to one recent study[1], a significant 58% of ALL malware attack victims are categorized as small businesses. In 2017 alone, these attacks cost small and medium-sized organizations an average of $2,235,000 per incident[2], once all costs associated with the damage or theft of IT assets and the disruption to normal business operations were accounted for. Based on all this, it should also come as a surprise to nobody that a full 60% of all businesses who suffer a cyber attack close their doors permanently within just six months[3].

The cyber security situation has literally never been more dire, especially if you own and operate a small business with under 50 employees. There's no getting around that fact. But luckily, this modern day problem also has a fairly straightforward solution. Because the fact of the matter is, regardless of how sophisticated an attack may be or how large it is in scope, almost 90% of them all begin in the exact same way:

With good, old fashioned human error. That's right: someone clicks on an email that they're not supposed to, accidentally logs into a fraudulent site posing as a legitimate one, or downloads and installs a file that ends up being a virus. Only 18% of attacks were driven by some type of external threat[4].

Therefore, if you want to make sure that this is the type of situation you do NOT find yourself in, there are a few key (and simple) steps that you can take today that will make all the difference tomorrow.

1 Everything Begins With An Actual Security Policy

Everyone knows that cyber security is important - but do your employees actually understand how important it is to your business? Do they know what they're supposed to do in order to protect your valuable data and assets, and what types of activities they should avoid? If the answer to those questions was "no," more often than not it's because your business doesn't actually have a hard and firm security policy to speak of. Therefore, the first step you can take today to reduce your business' chance of being hacked by 90% is simple:

Create one.

Get together with your IT staff and other key stakeholders and draft a comprehensive security policy for your employees to follow. As you do, make sure you're addressing all of the key factors, like:

- **Password retention.** Outline the rules governing what types of passwords can be created and how often they must be changed. Make it clear that people are not allowed to use the same password for different computers or devices. Make sure that people understand something like "firm123" is not a safe password and that they need to be using case sensitive passwords with combinations of numbers, letters and other special characters.
- **Have a policy regarding what software is allowed to be used on work computers.** This goes far beyond simply denying your employees the ability to "play games" on work time. Anything that is a potential threat has no business on your network.
- **Let people know when it's okay to bring their own devices to work and what rules they have to follow when they do.** Remember that any device connected to your network is a potential vulnerability just waiting to be taken advantage of. Now, realize that every smartphone or tablet an employee uses at work and at home could very well be that exploit and you'll begin to get an understanding of the situation you face.
- **Create a policy governing data access when someone changes positions, leaves your company voluntarily or gets fired.** People should have their account access revoked immediately to prevent unwanted access to key data moving forward.
- **Guest Wi-Fi.** Yes, you want your clients to have Internet access when they visit your office. But that shouldn't come at the expense of your security. You need to guarantee that anything connected to your network is safe.
- **Along the same lines, you should also create an update policy for software and hardware.** Make sure that all devices - including the hardware and the programs that run on it - are always updated to the latest versions to take advantage of bug fixes and security patches from the developer.

2 Training

Once you've created your security policy, you can move onto the next most important step for reducing your chances of being hacked: training your employees.

Keep in mind that this needs to go above and beyond just general awareness of cyber security best practices. Nobody wants to compromise your network, but mistakes can and often do happen.

People need to be trained about the latest types of threats that are out there, like how to spot a phishing email. Not only should they know NOT to click on suspicious links that they receive from unknown senders, but they also need to be aware of the very real consequences that they'll be subject to if they do.

If your employees aren't aware of the sophisticated types of attacks that are out there, they don't know what types of activities can get them into trouble. You could invest countless money into the latest anti-malware and anti-hacking tools that technology has to offer and it ultimately won't make a difference if someone still clicks on something they shouldn't because
they weren't thinking or weren't aware.

Likewise, this training needs to happen regularly - at least once a year, if not more. Hackers are always working to stay one step ahead of the curve, so you need to be proactive about staying ahead of them. All employees - both new hires and legacy employees - should go through this training on a regular basis.

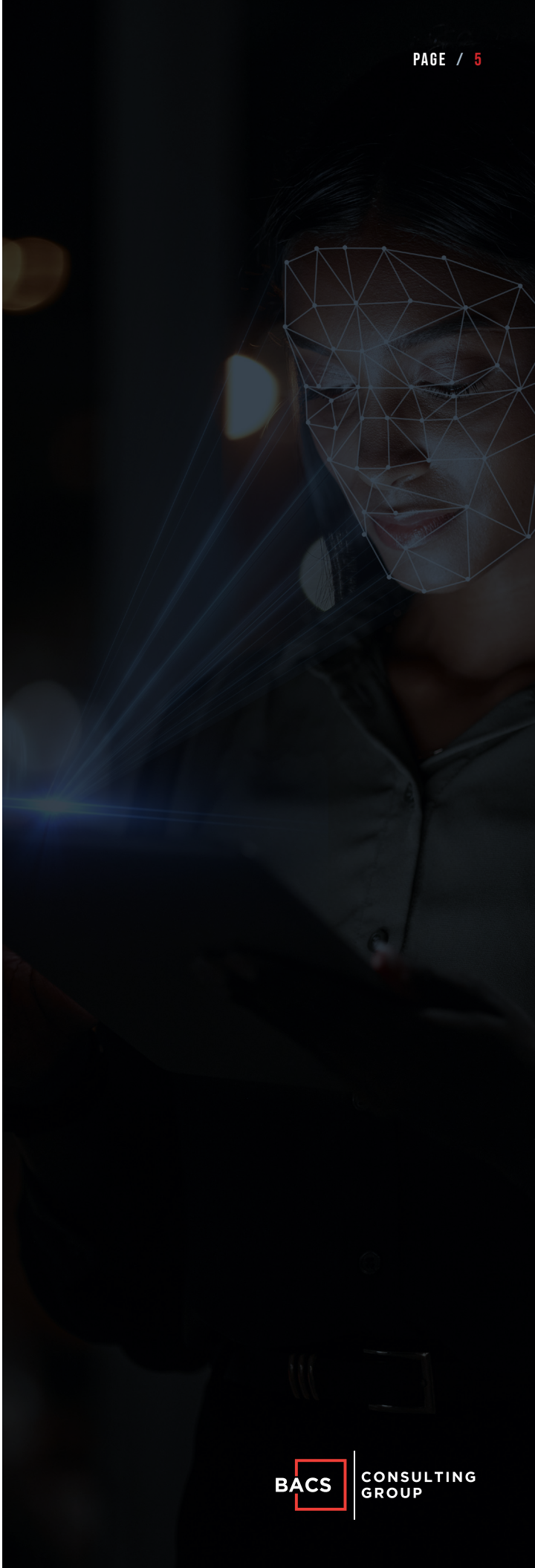
3 It's All About Access

Simply put, if someone does not need access to a particular networked folder or file to do their job, they shouldn't have access to it. End of story.

Because of this, the final thing you'll want to do to reduce your chances of being hacked by 90% involves totally re-thinking your file sharing policy, rebuilding it from the ground up.

Part of this feeds back into the security policy that you've created, but a large part of it is administrative. Engage with your employees to find out what resources they need access to and what data they need to effectively do their jobs every day. Then, partner with your IT team or your managed services provider to come up with actual user access policies to support that. Anything that ISN'T on that list isn't something a particular employee will be able to access.

Not only will this help prevent information from falling into the wrong hands, but it'll also mitigate risk in the event that you DO suffer a breach. It's hard to accidentally compromise your entire network if an affected employee never had access to it in the first place.



"Proactivity" Is the Name of the Game

At the end of the day, it's important for you to remember that true cybersecurity isn't just about having the latest and greatest firewall installed or using the most expensive IDS you can find. It's about being smart with the way your company uses the technological resources before you.

By creating an actual security policy, by training your employees and by re-thinking your approach to data access, you'll go a long way towards addressing the lion's share of the vulnerabilities that you'll be exposed to on an ongoing basis. At that point, you just need to remain proactive about protection. Find the gaps in your current system, see where you need improvement and act on that insight as often as you can.

The consequences are far too severe for anything less than that.

Sources

[1]https://enterprise.verizon.com/resources/reports/dbir/

[2]https://csrps.com/Media/Default/2017%20Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf

[3]https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

[4]https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

BACS CONSULTING GROUP

(650) 383-4248

INFO@BACSIT.COM

WWW.BACSIT.COM