EBOOK

Is Your Small Business

Truly Safe from Cybercrime?

Every Business is a Target of Cybercrime

PEGAS TECHNOLOGY SOLUTIONS LLC

71% **of the data breaches investigated by Verizon's forensic analysis unit targeted small businesses with fewer than 100 employees. Of that group, businesses with less than 10 employees were the most frequently attacked.**

According to a study conducted by Symantec, the number of cybercrime attacks targeting firms with fewer than 250 employees jumped from 18 percent in 2011 to 31 percent in 2012.

We always learn when large businesses (like Equifax) get breached. But when it comes to small and medium-sized businesses (SMBs) this goes unnoticed. This is ironic because SMBs are a primary target for cybercriminals. Why? —Because they are much easier to hack than a large enterprise. Here are some statistics that back this up:

According to the Ponemon Institute's 2nd Annual Cost of Cyber Crime Study, the average cost per breached record is between

$150 to $200.

The High Cost of Breaches for SMBs

Hackers usually go after confidential data like bank account info, credit card accounts and social security numbers. If your small business is breached, it will be costly. When the confidential data of your customers is exposed, they'll just take their business to your competitors. In many cases, this type of damaged reputation is irreparable.

You do the math. If you have 25 employees, you'll be hit with $5,000 in costs. This amount includes investigation and notification costs, litigation expenses, lost business, and the time it takes your staff to remediate the breach. The resulting consequences of cybercrime go well beyond the actual incident, and can have long-lasting implications.

Nearly two-thirds SMBs are out of business within six months after a breach. Small businesses simply can't withstand the affects from a breach the way large businesses like Target and Citibank can.

Plus, there are 47 state-specific DBN (Data Breach Notification) laws in the U.S. Laws and compliance regulations vary from state to state. A breach of customer data in Virginia will have different breach-notification requirements than California. If you serve customers in more than one state, this is a huge burden.

The 2012 State of Information Survey by Symantec revealed that nearly

50% of all SMBs

said a data breach damaged their reputation and drove customers away.

You Must Take Cybercrime Seriously.

If you're hit with a security breach, your customers may be less forgiving than you think. Many SMBs never regain their customers' trust.

Unfortunately, SMBs have become easy prey for cybercriminals — And the fact that there are so many small businesses makes them a prime target.

Plus, many owners of SMBs mistakenly view their data as trivial to hackers. They believe that large online businesses, big banks, and government entities are more attractive for hackers. The result? — They don't take cybersecurity seriously.

Today, cybercriminals prefer to hack small businesses, taking tiny bit of data over time so they aren't noticed. This can go on for weeks before it's discovered. If you're lax about implementing up-to-date protections, it's only a matter of time before your business is breached. You must change your way of thinking.

There are on average

1.29 cyberattacks

throughout the world every two minutes. The incidence is much greater in scope than the press reports.

Why Your SMB Is In the "Bull's Eye."

Large corporations can afford to use sophisticated security tactics to block most cybercrime attacks. The typical large business employs over 20 IT experts to ensure their network isn't breached. The cybercriminals know this, so they're focusing on small businesses instead.

Few SMBs have the full-time IT staff to monitor cyber threats. And even if they do, they're finding that their techs are overwhelmed with the tasks required to properly deal with them.

Cybercriminals also know that many small businesses can provide a pathway to larger, better-protected organizations. These small businesses are hired by larger companies as sub-contractors, or used as vendors for products.

Essentially, they're unknowingly acting as a "Trojan Horse" for hackers to gain backdoor access to the larger company's data. Hackers have developed malware to use on SMBs websites to get into the databases of their larger business partners. This is another reason why SMBs are the preferred target today.

The time has come to scrutinize your cybersecurity. In a survey of 1,000 SMBs,

over 66%

were sure that their data and devices were secure, when the opposite was true.
McAfee/ Office Depot

Staying Safe Is Good for Business.

What's happening today is that larger businesses are requiring their small-business partners to go through independent cybersecurity audits. (This is a good idea, regardless.) They are being carefully vetted by their larger partners to ensure they can be trusted with sensitive data.

If they can't prove that their network is secure, they'll simply be replaced by another business, and lose out on a potentially lucrative partnership.

Preventing Cyber Attacks Must Be Your Top Priority.

A comprehensive Cybersecurity Strategy can take time to implement. But, there are some things you can do right away to make your SMB safer from cyberattacks.

The following are 11 tips to help you get started.

1. Make a list of all the devices that connect to your network.

This includes laptops, tablets and smartphones. Every device that accesses your network must be properly secured. If your employees bring their own devices and use them for work, include them in your inventory as well. Determine if they're emailing work home to their personal computers and sending it back. An email to your network from their home computer that contains a virus can infect your entire network. This list should be reviewed and updated regularly to ensure every endpoint is secure.

2. Maintain your hardware and software with up-to-date patches and releases.

Developers release security patches whenever they become aware of vulnerabilities. Make sure all of your computers and applications are updated regularly.

3. Implement Mobile Device Monitoring (MDM).

Your IT provider can do this for you. They will approve or quarantine any new device that accesses your network, make sure they're encrypted, be sure they can be located at any time and place, and ensure they're remotely wiped of your sensitive company data if they're lost or stolen.

4. Use Tough Encryption.

While state and federal law requires businesses to use encryption to protect the sensitive information of customers, you should expand your use of encryption to include information that's not covered by compliance laws.

5. Ask Your IT Provider to Conduct Security Awareness Training for Your Employees.

Data breaches aren't always about bad people doing bad things. Many are the result of good employees making mistakes. If they aren't properly trained to recognize a cyber threat, your network and business are vulnerable.

According to the June 2013 Symantec Global Cost of a Data Breach Study, only

37% of data breaches are attributed to malicious attacks. The remaining 64% are causes by human and technology errors.

Phishing attacks manipulate employees into clicking malicious links where they're asked to provide login credentials. Make sure they know how to keep your company's data safe by avoiding common dangers like opening attachments from unknown senders, improperly disposing of sensitive information, or using simple passwords.

Every employee should participate in this training—And you should hold refresher courses, as threats are constantly changing.

6. Update Passwords Frequently.

Everyone's passwords should be frequently updated with a combination of numbers, lower case letters and special characters that can't be easily guessed. Or, make use of one of the popular Password Managers.

7. Write it Down.

It's important to have a written security policy for your employees that details best practices for both onsite and remote workers. Security policy training should be integrated your new-employee orientation. It should be updated periodically, and strictly enforced to be effective.

8. Back It Up.

Always backup your data each night to an offsite, secure location. The increased number of cyberattacks make frequent backups of critical data essential. You can back up your data manually or use a managed backup service.

9. Schedule an Independent Vulnerability Audit of Your Network.

If you want to keep your most sensitive business information secure, it's important to know exactly where it's stored. A detailed quarterly audit is recommended. A Vulnerability Audit determines if your technology is at risk from:

- Accidental deletions and human error
- Natural and manmade disasters
- Unauthorized access
- Data breaches
- Computer viruses and malware
- Hackers and cybercriminals

For a trusted and proven MSP contact Pegas Technology Solutions. We're your local cybersecurity experts.

Protect your small business — Schedule a Free Vulnerability Assessment by calling 207-835-4053 or emailing us at: sales@pegas.io

10. Review Your Outside Vendors.

It's common for small businesses to use third-party vendors for services like payroll or web hosting. If you do, make sure that all of your outside vendors have a comprehensive security plan in place to prevent hackers from accessing your private data.

11. Rely on Your MSP.

A Managed Service Provider (MSP) can handle all of your security measures. They'll be up to date on the latest cyber threats and solutions to protect your business. They can implement a multi-layered, managed security defense using sophisticated security devices, technical controls like firewalls, patching, antivirus, software updates, intrusion-detection and log analysis systems.

They can also provide your large-business partners a certified risk report outlining your security measures. This will satisfy your partners and instill confidence in prospective ones by proving to them that any potential security risks or vulnerabilities will be properly managed and addressed.