Checklist

Seven ways to protect your business network on a budget.

Small- and medium-sized businesses (SMBs) often don't think that hackers are interested in their affairs. But, that's far from the case. In fact, SMBs are prime targets because they inherently don't have the resources to patch up any sliver of an opportunity that hackers may find.

Just take a look at these findings from a 2018 survey by IDG and CDW:[1]

The new reality is that cyberattacks have become commonplace. And, not only are they growing, they're also increasing in complexity, severity and cost.

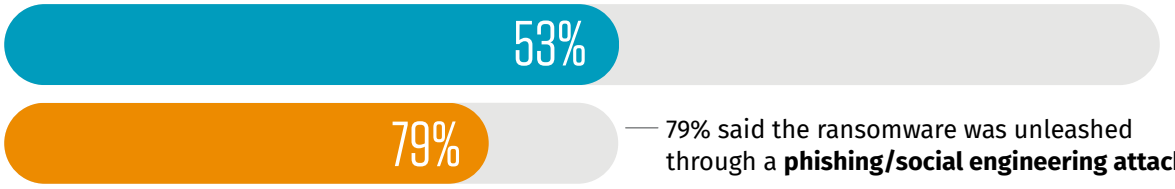
33%
of SMBs had purchased security software

25%
thought they were in compliance with the Payment Card Industry Data Security Standards (PCI-DSS)

30%
of IT leaders are confident they can thwart an attack against their business

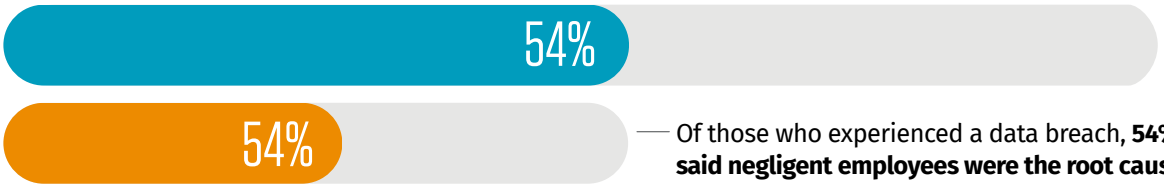
More than three of every five small- to medium-sized businesses were breached between 2016 and 2017, an increase from the year before.[2] Here's a deeper look at what types of cyberattacks have been hitting SMBs in recent years:[3]

53% of SMBs said they had more than two ransomware attacks — pieces of malware that block a victim's access to his or her files — in the last 12 months, significantly up from the 2 percent from the previous year



79% said the ransomware was unleashed through a **phishing/social engineering attack**

54% of SMBs said they had a **data breach involving sensitive information** about customers, target customers or employees in the last 12 months



Of those who experienced a data breach, **54% said negligent employees were the root cause**

Cyber attacks can seem even more unnerving when you look at the outcomes of businesses that have fallen prey: losses from the worst cases ranged from $84,000 to $148,000, and **60 percent of targeted SMBs shutter within six months of an attack.**[4]

The silver lining? Businesses don't need deep pockets or a large team of IT professionals to defend against cyberattacks. Use the checklist below to learn seven ways to protect your business network on a budget.

☐ Train employees on best security practices.

- Schedule mandatory interactive security training throughout the year instead of sending out security policies via email.
- Have and enforce a strict password policy, making employees create unique, strong passwords that are updated frequently.
- Require two-factor authentication, especially for applications that may house your most sensitive business data.
- Implement a company-wide policy for downloading and/or installing new software.
- Test your employees with mock phishing scenarios, and use the results to educate and increase awareness.
- Require encryption for employees who need to log in safely from another location.

☐ Have an IT resource completely focused on your network security.

- Whether an internal IT guru or an outsourced IT company, ensure there is someone whose sole job is protecting your network.
- Have that resource regularly audit your network, identifying vulnerabilities and finding solutions for them.

☐ Keep all software and router firmware updated.

- Use Software as a Service (SaaS), or cloud-based applications, which automatically update and patch security loopholes.
- Consider managed routers, which shift responsibility of router updates and protection to your service provider.

☐ Have firewalls.

- Add firewall protection on each computer and device.
- Include a network firewall to provide extra protection for anything attached to your corporate network.

☐ Secure your business Wi-Fi networks.

- Separate your guest Wi-Fi network from your back-office Wi-Fi.
- Mask your back-office Wi-Fi.
- Password protect your guest wireless network.
- Change the default password for all business Wi-Fi networks.

☐ Have antivirus/anti-malware protection on every business device.

- Run regular scans with your antivirus/anti-malware software.
- Pay for a supported version to get business-class protection.

☐ Invest in backups.

- Regularly back up your files, particularly the ones crucial to your business operations.
- Ideally, back them up more than once, storing them both physically on-site and off-site in cloud storage.
- Test your backups to ensure they are working and updating.

kinetic business
by windstream.

[1]https://biztechmagazine.com/article/2018/09/tech-small-businesses-need-prevent-data-breaches
[2]Ponemon Institute, 2017 State of Cybersecurity in Small and Medium-Sized Businesses
[3]Ponemon Institute, 2017 State of Cybersecurity in Small and Medium-Sized Businesses
[4]https://upscapital.com/product-services/cyber-liability-insurance/