SOPHOS
Cybersecurity evolved.

nutmeg CONSULTING

Secure Your Business From Cyberattacks

10 reasons small-medium businesses need better cybersecurity

Cyberattacks are being launched in the largest volume, and with more sophistication, than ever before. The increased competition amongst attackers means that more organizations are being targeted, with small and medium sized businesses (SMBs) no longer able to remain under the radar. In fact, the lack of resources and relatively weak defenses make SMBs an attractive target to a wide variety of threats.

10 reasons SMBs need better cybersecurity

1. Ransomware reigns supreme

No business is too small to evade a cyberattack. In fact, a recent Sophos global study found that over half of businesses were hit by a ransomware attack in the past year[1]. Most SMBs are also unable to recover from a ransomware attack that could cost over $500,000 to remediate.

2. The threat landscape evolves constantly

Small businesses must keep pace with the changing nature of cyber threats; however that is a full-time job and with hackers setting their sights on SMBs, cybersecurity needs to remain a top priority. In fact, the 2020 Verizon Data Breach Report notes a significant increase in phishing attempts targeting SMBs with the goal of obtaining credentials for monetary gain. Many SMBs concerned with the cost of fulltime IT security staff, can rely on MSPs to manage the tools that will protect them from threats.

3. A lack of IT hygiene

Maintaining IT hygiene, such as ensuring passwords are strong and changed regularly, will help reduce the risk of a breach. Businesses also need to review access rights to networks, files, and file shares to prevent adversaries from gaining access to sensitive data. A prescribed security solution from an MSP allows you to focus on your business while ensuring policies are in place to keep your workforce secure.

4. It's not a matter of 'If' you will get attacked, but 'when'

While it may seem logical that cyber attackers would focus their effort on targeting larger firms, the proportion of small firms (less than 50 employees) reporting one or more cybersecurity incidents is up from 33% to 47%[2]. Attackers typically target smaller businesses because they often lack up-to-date cybersecurity. Addressing this gap now will drastically increase your ability to stay protected in the future.

5. Keeping end users conditioned

Phishing, a type of social engineering tactic to steal data, passwords, and credentials remains a fruitful method for hackers being involved in 90% of breaches involving social actions in 2019[3]. This illustrates that end users are both the weakest link and the first line of defense for businesses. To prevent this threat, you should routinely test employees with simulated phishing attacks. Well-informed users can prevent threats like malware, ransomware, and more by being able to spot risks better.

6. Attackers are always looking for a weak point

Hackers typically will not stop if they find a locked door, instead they will try other entry points until they are in. Attackers can breach your environment through various channels including email, web browsers, mobile devices, and applications. Implementing a multi-layered security solution across your environment will ensure you are protected from a wide range of cyberattacks.

Work with a Sophos certified Managed Service Provider (MSP) to stay educated on the evolving threat landscape and the solutions you need to stay protected.

7. Next-gen attacks require next-gen solutions

Attackers are becoming increasingly more sophisticated every year. Businesses relying on out-of-date technology are far more likely to become victims of a cyberattack simply because hackers can easily bypass these older systems. Therefore,it is important to ensure your business is protected with industry leading next-gen tools that evolve to the latest cyberthreats.

8. Out-of-date systems = major vulnerabilities

In today's digital age you are likely to use tools that require regular updates and monitoring. Keeping these applications and tools updated can be onerous; however, by working with an MSP you can be assured that your systems are up-to-date and protected.

9. Network visibility is a blind spot

Having accurate information about your network, and what is connected to it, is vital in protecting it from both internal and external threats. Effective network monitoring tools can identify network anomalies and counter threats before they do damage. This visibility can help streamline internet usage and restrict unnecessary access for your users (such as blocking torrents, restricted websites, and more).

10. Staying compliant

For SMBs, compliance regulations require a range of cybersecurity protections and policies to be in place. Typically, laws and regulations like HIPPA and GDPR can be partially addressed through the implementation of next-gen security tools and end-user training. Working with an MSP can help you easily address these concerns and keep you compliant and secure.

Source:
1 Sophos The State of Ransomware 2020 Survey
2 2019 Hiscox Cyber Readiness Report
3 2020 Verizon Data Breach Report

To learn more about how **Nutmeg Consulting** can help secure your business from cyberthreats, please contact: **info@nutmegit.com**

Nutmeg Consulting, LLC
35 Philmack Drive B206
Middletown, CT 06457
860-256-4822

nutmegit.com
Email: info@nutmegit.com

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2021-01-07 (DD)