Top Six Cybersecurity Solutions for Every Business

As seen in the news every single day, cyber attacks are real and they are only going to increase as artificial intelligence (AI) enables the malicious actors to create more sophisticated attacks. The worst part is that they are specifically targeting small and midsized businesses (SMBs) knowing that their cyber defenses may not be ready for the daily assault. All organizations need to have a comprehensive cybersecurity plan and it needs to be more than just a "good" firewall and anti-virus. Most businesses are not sure what solutions are needed or what level of protection they need, because there are other factors that play into these decisions, such as budgets. CTS has effective cybersecurity solutions that are designed for every business regardless of industry or resources.

Top Six Cybersecurity Solutions for Every Business

1. Endpoint Detection and Response (EDR)

EDR solutions are behavioral AI engines that are built to detect and mitigate malicious code and scripts in documents and are capable of detecting fileless attacks and exploits. EDR provides rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

2. Backup Continuity and Disaster Recovery (BCDR)

BCDR goes beyond backup to enable rapid restoration of individual files or entire servers. Protecting from any type of disaster (going beyond simply recovering data), business continuity saves businesses by keeping them online in the face of otherwise devastating issues like ransomware, natural disasters, and costly human errors. With the ability to immediately get back up and running, BCDR solutions help you reduce disaster costs and avoid system downtime when it matters most.

3. Multi-Factor Authentication (MFA)

By requiring a second form of authentication, MFA is the best defense to strengthen access security and properly lockdown your Microsoft 365 e-mail from being compromised. MFA safeguards your systems when employees access externally facing systems, such as remote access via VPN or web-based portals.

4. SPAM and Anti-Phishing Email Protection

Protect and prevent sensitive data from leaving the organization and stop threats before they can enter your network through email. The native security features of most email solutions don't offer enough built-in protection to combat today's advanced threats — you should layer on third-party solutions that can provide advanced security features at both the server and mailbox levels.

5. Employee Security Awareness Training

A company's security posture is only as strong as their least secure employee. With phishing attempts growing ever-more-sophisticated, even savvy users can find themselves accidentally clicking malicious links, opening risky attachments, or mistaking a spoofed URL for a familiar website and giving sensitive information or credentials. Improve end user empowerment by engaging them with ongoing security training to teach them how to spot and respond to various types of threats.

6. Verified Patch Management

Every vendor regularly releases updates for their operating system or software including bug fixes, security updates, and improvements. It is important to manage these updates to make sure they are all installed and up to date and to control when they happen to avoid any disruptions to business continuity!

Top Six Cybersecurity Solutions for Every Business

Cybersecurity can be confusing and overwhelming, but it is essential for every business.

At CTS, we've developed a proven and cost-effective cybersecurity strategy for any business that actually works!

Consider the following statistics when thinking about whether you need protection for your business:

- An average of **2,244 cybersecurity attacks occur each day** according to a study by the University of Maryland.
- Blackberry reports that the United States remains the most highly targeted country with **65% of all cyberattacks targeting Americans.**
- According to Cybersecurity Ventures, **over 50% of all cybersecurity attacks target small to medium-sized businesses (SMBs).**
- Aside from costs a business may need to pay those behind a cybersecurity attack to get their data back, there are other significant costs a business may incur:
  - Between the 1st quarter of 2023 and the 3rd quarter of 2023, Statista reported that the average duration of downtime after a ransomware attack increased from 15 to 22 days.
  - A survey conducted by PricewaterhouseCoopers found that 87% of consumers consider changing who they conduct business with when a cyberattack occurs.
  - **Over 60% of SMBs that encounter a cyberattack, go out of business within 6 months** according to Cybersecurity Ventures.

Can your business afford to take a chance on not having proper Cybersecurity protection in place ?

If you're still unsure, consider the following example:
Business XYZ has 30 employees whose average annual salary and benefits package is $58,500 per employee, monthly operating and marketing costs of $6,500, and $4.8 million in gross sales. **If this business encounters a cybersecurity attack and loses just one day of business as a result, the cost is estimated to be at least $27,023!** As previously shared, compromised customer trust and attacks on business reputation carry costs and expenses difficult to recover.

To schedule a **FREE 30-minute** security discussion & assessment, contact **Frank Stephens** at **(847) 894-6304** or **fstephens@onlineCTS.com**.

onlineCTS.com
888.7.CTSNOW
info@onlineCTS.com
2033 N. Milwaukee Ave, Suite 351
Riverwoods, IL 60015