Project: Blog Post
Writer: Debby Wadsworth, Freelancer
SME: Dylan Kerling, VTS Technician

DW-writer.com
Debby@DW-writer.com
703-350-8508 cell

The following blog post was live from January 2022 to June 2022

How to Counter Cybersecurity Attacks

Cybercriminals delivered a wave of cyber-attacks in 2021 that were highly coordinated and far more advanced than ever. That year 576 US organizations fell victim to ransomware, and 34.1 million records were compromised. The downtime alone cost $159.4 billion, according to Comparitech. According to Cybercrime Magazine, cybercrime is predicted to cost the world $10.5 trillion annually by 2025.

Yet despite the numbers, the problem remains that U.S. companies are still not assigning a high priority to cybersecurity. Forbes reported in June 2022 that half of U.S. businesses still have not implemented a cybersecurity risk plan.

6 Steps for More Robust Cybersecurity

There are steps a business can take today to make its cybersecurity more robust until a risk plan is in place. The six steps are as follows.

Step 1: Education

Begin by creating and implementing an employee education program. Organizations are often affected by unaware or informed employees who click to open a link that unintentionally introduces malware into the network.

Step 2: Data Isolation - Air Gap Protection
Create an ‘Air Gap’ to isolate critical operational areas like accounting for your organization’s data system. An Air Gap can prevent further contamination if one system becomes infected.

Step 3: Continuous Monitoring, Testing, Upgrading
Continuously monitor and test your systems to detect potential intrusions or vulnerabilities early. Also, make sure there are no open doors or exploits that can enable unauthorized entry.

Step 4: Backup and Recovery
Make sure you have backup and recovery plans in place and are using them. The step may seem logical and automatic, but it is often incorrectly implemented, especially in the case of ransomware. Most backups are implemented as 2-1-1: 2 copies, 1 media type, and 1 location. Better still is a 3-2-1-1 backup strategy: 3 copies, 2 media types, 1 media location, 1 air-gapped copy.

Step 5: Improve Data Storage and Management
Basic protection plans with data backups are not enough in today’s war on security. Continuously monitoring IT infrastructure is essential to catch potential hardware or software failures and detect threats and intrusions from inside and outside the company, including customer portals.

Step 6: Improve Data Security
Move to a higher level of data security by upgrading or adding things like hybrid cloud storage that prevent ransomware attacks.

For more ways to effectively manage cybersecurity, visit VTS.com/blog

--end--