Valley Expetec

End-of-Year Cybersecurity Health Check
Guide for Business Owners

Assess And Strengthen Your Business's Cybersecurity Before 2025



Introduction

Another year is coming to an end. As such, it's an ideal time to take a step back and examine the state of your company's cybersecurity health. Now more than ever, cybersecurity plays a crucial role in protecting your digital assets and ensuring the continuous growth and success of your establishment. It is therefore a wonderful thing that you are taking an interest in keeping an eye on the performance of your cybersecurity solutions.

But how do you begin? Which areas should you prioritize? What questions should you ask? This is not something that they teach you in business school!

The process can all be overwhelming, especially for a non-techie. However, with this simple guide, you won't have to hide in the dark. Just follow the steps and you will be able to make your own thorough assessment of your existing cybersecurity measures and identify the necessary steps to make them even more efficient for the coming year.

Why You Need This Cybersecurity Health Check?

Cybersecurity risks continue to increase each day, and there's no telling who could be the next victim. For all you know, it could be you. Even if you are confident in your security measures, unfortunately, there is no such thing as full immunity. And that is why you need this cybersecurity health check.

The global average cost of a data breach in 2024 is USD 4.88 million - IBM.com

A single data breach can result in massive expenses, often amounting to millions of dollars. It can also cause a significant loss of clients and a majorly damaged reputation for your business.

With the help of this guide, you can conduct a quick but thorough health check of your cybersecurity system. It will help you identify weak areas and plan contingencies to boost your defenses, just in time for the new year.

CYBERSECURITY THREAT CHECKLIST

There are several areas that you need to closely examine to arrive at an accurate assessment of your company's cybersecurity health. In fact, some of these vulnerabilities might not even seem like an issue to you, but they are. So, go through this list carefully and check all the items that you feel need to be improved.

1 CYBERSECURITY POLICIES

- [ ] Does your company have a formal cybersecurity policy in place?
- [ ] Is your cybersecurity policy periodically reviewed and updated as necessary?
- [ ] Is there a dedicated IT team or individual that is responsible for the company’s cybersecurity?
- [ ] Are all members of the organization aware of the cybersecurity policies and are required to follow them at all times?

2 EMPLOYEES

- [ ] Does your company provide regular cybersecurity awareness and data security training for employees?
- [ ] Are the employees trained to identify suspicious emails and recognize phishing attempts, and report these incidents immediately?
- [ ] Do you monitor employees for proper use of cybersecurity measures for daily operations?
- [ ] During onboarding and offboarding employees, are cybersecurity concerns specifically addressed?

3 HARDWARE AND SOFTWARE

- [ ] Do you properly dispose of old hardware that no longer gets security updates and replace it with newer equipment?
- [ ] Are mobile devices properly secured before being used to access internal data?
- [ ] Do you always update software and mobile apps when a new version is released?
- [ ] Do you verify if the software comes from trusted sources before being allowed in the system?

4 DATA SECURITY

- [ ] Do you use reliable encryption methods for data while in storage?
- [ ] Do you use reliable encryption methods for data while in transit?
- [ ] Do you have a data classification system to identify and protect sensitive information?
- [ ] Are backups of critical business data performed on a regular basis?
- [ ] Do you implement strict policies for the management and protection of Personal Identifiable Information (PII)?
- [ ] Are the cloud solutions used for data storage protected with encryption and authentication controls?
- [ ] Is there a reliable Data Loss Prevention (DLP) solution in place to facilitate the secure transfer of sensitive data?

5 ACCESS CONTROL

- [ ] Do you and your employees use strong, hard-to-decipher passwords?
- [ ] Are employees required to change or update passwords after a certain period to minimize the risk of compromise?

- [ ] Do you use multi-factor authentication during the login process?
- [ ] Is access to sensitive information restricted to employees who need it to do their jobs?
- [ ] Do you maintain data access logs for the purpose of tracking potential breaches?
- [ ] Is network traffic constantly monitored to detect suspicious activities?
- [ ] Are user accounts temporarily disabled after a certain number of failed attempts to prevent unauthorized entry?

6 VIRUS & MALWARE

- [ ] Do you have antivirus and anti-malware programs installed on all endpoints?
- [ ] Are automatic updates enabled for anti-malware solutions so new threats can be detected?
- [ ] Do you perform an automatic scan of all files when they enter the system?
- [ ] Are employees trained not to download files or apps from unverified sources?
- [ ] Are vulnerability assessments and penetration tests regularly conducted to check the system's defenses?

7 NETWORK SECURITY

- [ ] Do you have firewalls in place and configured properly, with permissions restricted to authorized personnel only?
- [ ] Do you require employees to use VPN protection when accessing company data from remote locations?
- [ ] Are all ports being monitored to prevent exposure of internal systems to outside threats?
- [ ] Do you have a reliable intrusion detection system in place to detect potential attacks?

- [ ] Is network traffic constantly monitored to detect suspicious activities?
- [ ] Are security patches and other critical updates applied as soon as they are available?
- [ ] Is your network segmented into multiple smaller networks to better contain a data breach in case it occurs?

8 INCIDENT RESPONSE

- [ ] Does your company have a prepared incident response and recovery plan for handling data breaches?
- [ ] If so, is the incident response plan ready to deploy as soon as a security breach occurs?
- [ ] Does the incident response plan include a complete list of procedures and roles that cover detection, response, and recovery from cyber incidents?
- [ ] Is every employee who has an active role in the incident response plan aware of their role and able to implement it at any time?
- [ ] Are simulations or drills for testing the company's incident response plan periodically conducted?

9 THIRD-PARTY & VENDOR SECURITY

- [ ] Are third-party vendors meticulously evaluated for cybersecurity practices before being allowed into the system?
- [ ] Are Service Level Agreements (SLA) incorporated with vendor contracts to specify the required security level and indicate penalties?
- [ ] Is data sharing with external partners limited to the absolute minimal amount necessary for them to do their job?
- [ ] Are strict precautions being implemented to prevent threats with fourth-party risks?

10 PHYSICAL SECURITY

- [ ] Are all company computers kept in a secure location where only authorized employees can get access?
- [ ] Is confidential information protected from leaving the organization by disabling USB ports and similar measures?
- [ ] Are printed copies of sensitive data shredded when no longer needed?
- [ ] Are security cameras used to monitor server rooms and other areas where sensitive information is stored?
- [ ] Does your company use key cards, biometric scanners, and access codes to control access to facilities?



RISK SCORING TOOL

After going through the checklist and ticking off the items that you feel you have accomplished, it's now time to take a more in-depth analysis and score your risks. Considering your responses in the checklist and the level that you think your organization has addressed each of these vulnerabilities, rate each of the areas below on a scale of 1 to 5, where 1 indicates that you are fully confident of your protection, and 5 means you're seriously at risk.

Area of Vulnerability	1	2	3	4	5
Cybersecurity Policies					
Employee Awareness					
Hardware and Software Security					
Data Security					
Access Control					
Virus & Malware Protection					
Network Security					
Incident Response					
Third-Party & Vendor Security					
Physical Security					

INTERPRETING YOUR TOTAL RISK

1-10: You're doing very well, but some areas might still be enhanced.

11-20: You're still in pretty good shape but prevention is better so it's recommended that you consider some tweaks.

21-30: You're pretty much like most businesses, with some good areas but also some that need urgent action.

31-40: There are several red flags in your cybersecurity and you need to fix them soon.

41-50: You're at serious risk and must take immediate action!

REMEDIATION TIPS



Enable Multi-Factor Authentication

Adding multiple levels of security, like SMS codes sent to your phone, guarantees that accounts remain secure even though passwords might be compromised.



Conduct Security Audits

Regular audits and testing of security measures can reveal weak areas before cybercriminals discover them, giving you the chance to fix vulnerabilities before the risk escalates.



Train Your Employees

Educating your staff on identifying phishing emails, recognizing social engineering tactics, and practicing security measures can make a vast difference.



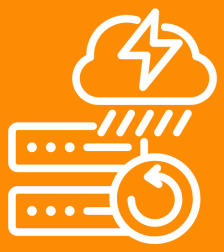
Limit Access Control

Using a role-based access control (RBAC) is very effective in keeping sensitive information within the confines of the system and preventing insider threats.



Update Your Software

When a new software version or a new security patch is released, be sure to make the updates as soon as possible to keep your system protected against newly discovered threats.



Have a Data Backup and Recovery Plan

In the event of a cyberattack, critical data should always be backed up and stored in a secure location, allowing you to facilitate a quick and efficient recovery.



Schedule an MSP Consultation

Managed Service Providers can do so much more for your cybersecurity than an in-house team can, like easy access to expert advice and state-of-the-art security tools.

When to Bring in the Experts

Did you get a troubling risk score? Or maybe you scored well but still want assurance about the security of your business. Either way, consulting with an MSP would do you a lot of good.

Our team consists of highly trained specialists with decades of experience in IT security, fully capable of providing expert advice on all your cybersecurity concerns. We also have extensive access to the most advanced tools and solutions in cybersecurity today.

With all the resources that we can make available for you, your business is certain to get the highest protection against any cyber threats.

Take control of your cybersecurity today.

With the help of this guide, you are taking the very important first step towards keeping your business safe and ensuring that your data and network are fully protected as you step into **2025**.

Need help or have further questions?

Contact Valley Expetec today and **schedule a free consultation!**

