CYBERSECURITY CHECKLIST

The purpose of this evaluation is to make you aware of cybersecurity issues your organization might have missed. Cybersecurity is only as good as the weakest link in the process.

The following checklist is based on an industry-recognized list of the most critical security controls [1]. Your organization might not need to implement every control, but it's important to evaluate the possible risks and potential impacts of not doing so. Checkmark the box if you can answer yes to these questions.

☐ **Do you have accurate and real-time knowledge of all devices connected to your network?**

Timely identification of unauthorized and unmanaged devices is critical for protection of organizational networks. Accurate inventories of managed devices allow for proper maintenance, backup and cyber hygiene. Mobile devices (such as laptop computers) are frequently targeted by attackers and can be an easy way into your organization's network.

☐ **Do you have accurate and real-time knowledge of all software your employees are running on the network?**

Unpatched and uncontrolled software is easy to compromise and remains one of the most common sources of cybersecurity incidents. Knowing what software is running on your network helps your organization properly manage patches and known vulnerabilities and, at the same time, allows you to easily identify rogue applications and prevent security compromises.

☐ **Do you have a malicious software defense strategy?**

Malicious code (a.k.a. viruses) can spread rapidly and enter computer networks through various entry points. Proper planning of anti-malware controls is essential for maintenance of cyber hygiene.

☐ **Do you develop secure configurations and enforce them on IT resources connecting to your networks?**

Common applications running on your network contain hundreds of thousands of settings that can easily be overlooked or changed during the update process and eventually leave open backdoors into your network. As new security vulnerabilities are discovered, new and additional settings may need to be changed. Proper configuration and change management processes help organizations minimize the network downtime.

☐ **Do you continuously assess the IT landscape for vulnerabilities and remediate them in a pre-defined time period?**

New vulnerabilities in software and hardware running on your network are discovered daily, sometimes even hourly. Constant monitoring and proper remediation and mitigation are key for safe operations of your IT infrastructure.

☐ **Do you ensure your in-house developed applications are free of vulnerabilities?**

Cyber security attacks frequently come through web based applications. Application developers are rarely properly trained in secure coding and are not in the security business; their job is to get the code working. The only way to prevent software vulnerabilities and avoid cyber incident is to implement and manage proper secure lifecycle for all in-house developed code.

Continued on next page ...

[1] *Critical Security Controls for Effective Cyber Defense (https://www.sans.org/critical-security-controls/)*

CYBERSECURITY CHECKLIST

☐ **Do you have full control of your organizational wireless networks?**

Your employees love them. Unfortunately, so do the bad guys. Wireless networks allow them to access your resources without even being physically connected to your premises. Proper management, control and monitoring of wireless networks are key for having full control over your infrastructure.

☐ **Do you know your data recovery capability?**

According to a study from Price Waterhouse Coopers, 70 percent of small firms that experience a major data loss go out of business within a year. And yet, most small organizations still do not have proper controls in place. When was the last time your organization conducted a full data recovery exercise? A strong data recovery capability does not have to be expensive and is within a reach of even the smallest organizations.

☐ **Do you have mandatory security awareness training for your staff? (If so, how often?)**

Overall security of any organization is only as good as the weakest link in the entire process. Frequently neglected, the end-users play a critical role in organizational security. Strong cyber defense starts with your key asset: people.

☐ **Does your organization limit and control network ports, protocols and services?**

Attackers are constantly on the lookout for entry points into your network. Limiting open ports and available protocols and services to only those that are essential to functionality is not only one of the best practices but also essential for minimizing your attack surface and exposure.

☐ **Do you know your system administrators?**

The principal method for an attacker to move around your network once they gain access is through misuse or elevation of access privilege. Not every user in your organization should be a system administrator. The principle of the least privilege is one of the core principles in cybersecurity. Elevated (administrative) privileges must be tightly controlled and granted to only a few people.

☐ **Do you know your boundaries?**

Without clearly defined boundaries and knowledge of your assets, all your security efforts will be useless. With proliferation of mobile technologies, boundaries are becoming increasingly more difficult to define and control.

☐ **Do you know where your audit logs are?**

Attackers and malicious code thrive in environments without audit logs where they can remain unnoticed for a very long time. Even when such activities are discovered, it is impossible to determine the extent of the damage or conduct forensic investigations without proper audit trails.

☐ **Do you know who determines who has access to what assets and why?**

In some of the highest profile security breaches in the news in the last few months, attackers gained access to the most sensitive assets that were stored together with less critical and lower value data. Sensitive assets do not always mean secrets.

☐ **Do you actively manage user accounts?**

Dormant and expired user accounts are frequently misused by attackers. Proper account management process is critical in order to have full control over who has access to what, when and how. Disgruntled employees with active accounts, or with knowledge of other coworkers' credentials, can be more dangerous than the most sophisticated hackers.

☐ **Do you identify and protect your sensitive data?**

Remember, sensitive information does not equate to secrets. Your organization might not have any secrets, in fact all your work may be completely public, but you will still maintain a trove of sensitive information in various places, possibly even in the cloud. Integrity and availability of your valuable data must be properly protected.

Continued on next page ...

CYBERSECURITY CHECKLIST

☐ **Is your incident response management program working?**

Even the best security practices cannot completely eliminate the possibility of a cybersecurity incident. When such incidents occur, the reputation of your organization is at stake and it's too late to plan your next move. A proper incident response program must be developed and managed long before incidents occur. It is not an option!

☐ **Is your computer network engineered in a secure manner?**

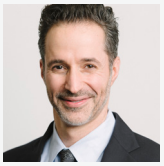
Most computer networks in operation today evolved from some small office/home brewed computer setup and are not architected with security in mind. Even those that did are constantly evolving and require constant attention. Security cannot be an afterthought. It must be built in from the very conception of the organization.

☐ **Has your organization recently conducted an attack exercise?**

Often called (pen)etration tests or red team exercises, these are critical to identify gaps in any cybersecurity initiatives. Every organization needs to periodically test its defenses to find the vulnerabilities before the bad guys do.

Ready to make your organization more secure? Call or email us for a free security consultation to help you identify your next steps.

CONTACT US



Frederic Persi (CPA)
IT Services - Partner
(703) 253-9721
fpersi@apextechllc.com

Branko Bokan
Cybersecurity - Director
(703) 253-9731
bbokan@apextechllc.com