

## Quick List – 12 Cybersecurity Controls

1. Multi-factor Authentication for remote access, email access, and admin/privilege controls
2. Endpoint Detection and Response (EDR)
3. Secured/encrypted and tested backups
4. Privilege Access Management (PAM)
5. Email filtering and web security
6. Patch Management & Vulnerability Management
7. Cyber incident response planning & testing
8. Cybersecurity awareness training and phishing testing
9. Hardening techniques, including Remote Desktop Proposals (RDP mitigation)
10. Logging and monitoring/network protections
11. End-of-Life systems replaced or protected
12. Vendor/digital supply chain risk management

### 1. Enable Multifactor Authentication for ALL Users

Multifactor authentication (MFA) is a critical security control to reduce risk across an enterprise. An organization can significantly reduce phishing attempts, credential stuffing attacks, and ransomware incidents by ensuring that users use not only a password but also a secure token. MFA should be enabled for email, VPN, and critical system access.

### 2. Create and Continuously Test an Incident Response Plan

An incident response plan is an effective way to identify, respond to, and recover from cybersecurity incidents. Incident response plans contain details about classifying, triaging, and escalating security incidents to critical contacts who oversee and manage an incident.

However, a document that sits on a shelf collecting dust does no good. An incident response plan must be regularly tested with real-world

scenarios or tabletop exercises to be effective. Involve key stakeholders and those who support the incident management team to ensure the plan is accurate and assists in adequately resolving any incident. An established incident response plan is also a critical aspect of security and audit frameworks, including PCI-DSS, NIST, and ISO-27001

### 3. Explicitly block remote access ports at the firewall or network gateway (e.g., remote desktop protocol)

In ransomware cases, one of the most abused protocols on the internet is allowing Remote Desktop access from the public internet to the internal network. By implementing a VPN, remote access gateway, or other network filtering device (in addition to the MFA requirement), an organization can significantly reduce the chances of a ransomware attack.

It is not enough to simply reassign Remote Desktop to a non-standard port (3389). Threat actors scan for all available ports, and for them, identifying remote desktop protocol (RDP) on a non-standard port is trivial, and it offers an organization no additional protection.

The only way to reliably secure RDP on the internet is to put it inside a VPN. Therefore, the best practice is to not expose RDP to the internet at all.

### 4. Air Gap & Encrypt Backups

Simply having backups is no longer enough to thwart threat actors. Organizations must encrypt backups and, ideally, store them in an air-gapped environment. If backups are encrypted, threat actors will have more difficulty accessing or altering sensitive files once they establish initial access. By taking the extra step to air gap, an organization can be reasonably sure

that the data it maintains is out of reach of almost any threat actor who does not have physical access.

Air gapping and encryption are only half the battle, though. An organization must regularly test backups with a file-by-file spot check and complete restoration events to manage backups effectively. What's more, by logging metrics from these events, an organization can fully understand the potential impact of a catastrophic event when the full restoration is needed.

### 5. Use Email Filtering & Web Security

Starting from the outside, let's look at DMARC, SPF, and DKIM. These protocols attached to an organization's external MX records prevent impersonation of its domain and man-in-the-middle attacks. Anyone with an internet connection can easily verify if these are in place.

Click on the wrong email or web link, and someone is inside your perimeter controls. Thus, employ email security gateway protection to prevent unwanted emails and deliver good ones. This reduces spam, phishing attacks, malware, and fraudulent content — like a firewall for email. In the same way, web filters (aka URL filters) will eliminate known bad content and significantly reduce suspect content.

Security education and awareness regarding these two issues are critical and, in the long run, the most cost-effective way to deal with this prevalent risk.

### 6. Remove End-of-Life (EOL) and End-of-Support (EOS) Devices and Software

One of the most difficult tasks for many organizations is proper patch and vulnerability management. Attackers commonly target these “legacy” systems, which organizations are no longer patching and addressing security issues on. For mission-critical systems that cannot be upgraded or migrated to newer methods, enable additional

compensating controls for proper alerting on malicious behaviors and strict access management.

Legacy systems, such as Windows 2003, XP, and Server 2008 R2, are examples of end-of-life operating systems. While heavily utilized by many organizations, they add risk because the vendors are no longer releasing security patches for these systems.

## 7. Implement advanced endpoint detection and response solutions on all endpoints and servers

Endpoint detection and response (EDR) solutions can be instrumental in preventing ransomware and other malicious activities, such as credential dumping and network reconnaissance. Many EDR solutions leverage machine learning to identify and prevent malware from executing, even if the malware has never been identified. This type of behavioral analysis is very effective at preventing threat actors from loading their toolsets.

Another advantage of EDR solutions is that they provide security analysts with significantly more details — not just about the file that was blocked but also the process trajectories and user activities leading up to the event. They also offer various options for mitigating threats.

## 8. Enable logging for all systems, software, and perimeter devices

A common issue during incident response and digital forensics engagements is a lack of available logging and evidence. Endpoints, servers, and network equipment often have capabilities to not only generate logs but also send them to a centralized logging platform or Security Incident Event Manager (SIEM) for storage and threat correlation.

These technologies allow for preservation of important logs for analysis in the event of an incident.

In many cases, organizations have not configured these logs for storage, and since the storage space by default is very low, important log data and artifacts cannot be reviewed because the logs have been overwritten. A retention period of at least 90 days for all security event logs, network perimeter devices, and remote access devices is a best practice.

### **9. Conduct employee awareness training and phishing simulation**

Threat actors are continually creating highly sophisticated methods of phishing and fraudulent activities against unsuspecting employees. Not every employee will be tech-savvy. Security awareness training helps employees understand the real-world risks of phishing and social-engineering attacks. By providing tools to train employees, an organization can reduce the likelihood of a threat actor successfully exploiting the human aspect of security.

### **10. Update patch management programs**

A modern patching program should include policies and mechanisms to manage software updates promptly. Patching efforts should address operating system updates and commonly utilized software within the environment. An active patching plan should aim to reduce the mean time to patch and provide metrics on existing patch efforts.

In the event of a high-severity vulnerability, a mature patching program should also be able to identify the risks and exposure for a given set of systems based on the average time to patch. This will help key stakeholders make critical decisions when a new exploit is released.

### **11. Deploy password managers and adopt least-privilege access**

Password managers can significantly reduce the risk of weak password usage among employees. By implementing an organization-wide

password manager, employees can generate strong, unique passwords for each site they need to access. Since password reuse is a common issue, users can quickly adopt better password standards at work and at home. Password managers often implement MFA to ensure proper ownership of the account. The use of password managers can also lead to a reduction in support costs associated with password resets in the event a user cannot remember their password.

The concept of “least-privilege access” is a common technique to ensure that each user account only has access to that which is explicitly needed. Users should not have access to systems and applications that are not directly related to their day-to-day responsibilities. By restricting administrative access, organizations can significantly reduce the risk of a threat actor compromising an account and gaining access to the data they need. Administrators must have a second, dedicated admin account that requires MFA for each administrative task. To be clear, these administrative accounts are in addition to their user accounts.

## 12. Manage and secure the vendor/digital supply chain

Using older or unpatched versions of any software carries risks, but those management applications make organizations especially vulnerable. Recent IT management software exploits have highlighted that IT departments can use their tools against them. Perfect examples are the SolarWinds, Kaseya, and Log4J breaches.

The solution? Upgrade and patch. And when done, upgrade and patch again. Make this a habit.

Security begins at contract time. Good security language in software contracts is important, but what’s more important is good security intelligence, which keeps awareness high regarding anything in an organization’s supply chain. IT must stay aware of vulnerable programs and have the means to react promptly and remediate them.

