MarshMcLennan Agency | Arete

# 12 Security Controls Recommended by Cyber Insurers

The current cyber insurance marketplace for all insureds has shifted dramatically due to the increased frequency and severity of security and privacy claims over the past year, including more sophisticated ransomware events, business email compromises, supply chain disruptions, and social engineering attacks.

Many leading cyber insurers have imposed minimum security control requirements in order to provide Cyber insurance coverage terms. **MMA** has partnered with **Arete Advisors** to summarize these top 12 cyber security hygiene recommendations to help improve your cyber security posture and better prepare your organization for the cyber insurance marketplace. MMA's **Cyber Resiliency Network (CRN)** is available to MMA clients to directly assist in consulting on these best practices. For more information, please visit our CRN webpage here.

## Quick hit list of 12 security controls for the insured

1. Enable multifactor authentication
2. Create and continuously test an incident response plan
3. Explicitly block remote access ports at the firewall or network gateway (e.g., remote desktop protocol)
4. Air gap and encrypt backups
5. Use email filtering and web security
6. Remove end-of-life (EOL) and end-of-support (EOS) devices and software
7. Implement advanced endpoint detection and response solutions on all endpoints and servers
8. Enable logging for all systems, software, and perimeter devices
9. Conduct employee awareness training and phishing simulation
10. Update patch management programs
11. Deploy password managers and adopt least-privilege access
12. Manage and secure the vendor/digital supply chain

## 1. Enable multifactor authentication for all users

Multifactor authentication (MFA) is a critical security control to reduce risk across an enterprise. By ensuring that users not only use a password, but also a secure token, an organization can significantly reduce phishing attempts, credential stuffing attacks, and ransomware incidents. 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 how to classify, triage, and escalate security incidents to critical contacts who oversee and manage an incident.

However, a document that sits on a shelf collecting dust does no one any good. To be effective, an incident response plan must be regularly tested with either real-world scenarios or tabletop exercises. Involve key stakeholders and those who support the incident management team to ensure the plan is accurate and assists in the proper resolution of 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 and 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 a harder time accessing or altering sensitive files once they establish initial access. By taking the extra step to air gap, an organization can be reasonably certain that the data it is maintaining is out of reach of almost any threat actor who does not have physical access.

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

## 5. Use email filtering and web security

Starting from the outside, let’s look at DMARC, SPF, and DKIM. These are protocols attached to an organization’s external MX records that 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, which is designed to prevent unwanted email and deliver good email. 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 is 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 systems, enable additional compensating controls to allow for proper alerting on malicious behaviors as well as 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. Security awareness training helps employees understand the real-world risks of phishing and social-engineering attacks. Not every employee is going to be tech savvy, and 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 in a timely manner. Patching efforts should address not just operating system updates, but also 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 such a common issue, this can make it easy for users to adopt better password standards at work and at home. Password managers often implement MFA to ensure proper ownership of the account. 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. A user 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

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

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 promptly react and remediate.

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affected if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change. d/b/a in California as Marsh & McLennan Insurance Agency LLC; CA Insurance Lic: 0H18131. MarshMMA.com

MarshMcLennan Agency
A business of Marsh McLennan