MarshMcLennan Agency | Arete | PayneWest INSURANCE
A Marsh & McLennan Agency LLC company

10 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 10 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 brochure here.

Quick Hit List of 10 Security Controls for the Insured

1. Multi-factor authentication (MFA) (remote access, admin access, email, critical systems, vendor access, etc.)
2. A current and tested incident response plan
3. No open ports for remote access (e.g., Remote Desktop Protocol (RDP))
4. Air-gapped and encrypted backups, including the demonstrated ability to test and restore from backups
5. The sunsetting or removal of end-of-life software
6. The presence of an advanced endpoint detection and response (EDR) solution
7. Enabled logging for all systems, software, and perimeter devices
8. Employee awareness trainings and phishing simulations
9. An updated patch management program
10. A password manager/vault and adoption of least privilege access

MarshMcLennan Agency | Arete | PayneWest INSURANCE
A Marsh & McLennan Agency LLC company

1. Enable multi-factor authentication (MFA) for all users.

MFA is a critical security control to reduce risk across an enterprise. Ensure users not only know a password, but also possess a secure token. This 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 consistently test an incident response plan.

An incident response plan is an effective way to identify, respond, and recover from cybersecurity incidents. Incident response plans contain details about how to classify, triage, and escalate security incidents to the critical contacts that oversee and manage an incident.

A document that sits on the shelf collecting dust does no one any good though. An effective incident response plan should be tested regularly with either real world scenarios or tabletop exercises. Key stakeholders and those that support the incident management team should be involved to ensure the incident response plan is accurate and assists in the proper resolution of any incident. Having 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 (RDP).

One of the most abused protocols on the Internet in ransomware cases is allowing Remote Desktop access from the public internet to internal network. By implementing a VPN, remote access gateway, or other network filtering device (in addition to the MFA requirement), chances for a ransomware attack are significantly reduced.

It is not enough to just reassign Remote Desktop to a non-standard port (3389). Threat actors scan for all available ports and identifying RDP on a non-standard port is trivial and offers no additional protections.

4. Create air-gapped and encrypted backups.

Simply having backups is not enough to thwart threat actors any longer. Backups need to be encrypted, and ideally also stored in an air-gapped environment. By encrypting backups, threat actors will be less likely to be able to access or alter sensitive files once initial access has been established. By taking the extra step of an air gap, an organization can be reasonably sure that the data they are maintaining is out of reach for almost any threat actor without physical access.

This is only half of the battle though. In order to effectively manage backups, the backups must be tested regularly, both with a file-by-file spot-check, as well as complete restoration events. Metrics from these events should be logged so that an organization can properly understand the potential impact of a catastrophic event in which a full restoration is needed.

5. Sunset or remove end-of-life (EOL) and end-of-support (EOS) devices and software.

One of the most difficult tasks for many organizations to tackle is proper patch and vulnerability management. Attackers commonly target these "legacy" systems as it is well known that patches and security issues are no longer being addressed. For mission-critical systems that are unable to be upgraded or migrated to newer systems, additional compensating controls should be enabled to allow for proper alerting on malicious behaviors as well as strict access management.

Legacy operating systems such as Windows 2003, XP, and Server 2008 R2 are examples of end-of-life operating systems. These are heavily utilized by many organizations, but additional risk is introduced because security patches are no longer being released for these systems.

6. Implement advanced endpoint detection and response (EDR) solutions on all endpoints and servers.

The presence of an EDR solution can be instrumental in preventing ransomware and other malicious activities such as credential dumping and network reconnaissance. Many of these EDR solutions leverage machine learning to identify and prevent malware from executing, even if it has never been identified before. This behavioral analysis is very effective at preventing threat actors from loading their tool-sets.

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

7. 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 to 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, Arete encounters situations where the client has 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. Arete recommends a retention period of at least 90 days for all security event logs, network perimeter devices, and remote access devices.

8. Conduct employee awareness trainings and phishing simulations.

Threat actors are continually creating highly sophisticated methods of phishing and fraudulent activities against unsuspecting employees. Employee awareness training helps the 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.

9. Implement an up to date patch management program.

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 level updates, but also commonly utilized software within the environment. An active patching plan should aim to reduce the mean time to patch, as well as provide metrics on existing patch efforts. A mature patching program should be able to identify the risks and exposure for a given set of systems based on the average time to patch in the event of a high-severity vulnerability. This helps key stakeholders make critical decisions when a new exploit is released.

10. Deploy a password manager and adopt least privilege access.

Password managers can significantly reduce 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 access to. 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. Usage 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 to users, the risk of a threat actor having compromised an account as well as having access to the data they need is significantly reduced.

A business of Marsh McLennan

Your future is limitless.℠