MOXFIVE

DATA SHEET

Business Resilience
Starting the Journey

Improving Cybersecurity Resilience

A significant cybersecurity incident is not only a business crisis: it can also become a powerful catalyst for enhancing fundamental IT capabilities. A growing universe of products and service providers compete for your attention to be included in the plan. Not only are cyber insurance premiums increasing, but insurance carriers are also tightening underwriting rules to require specific controls that mitigate the impact of attacks.

MOXFIVE is ready to help you implement measures that will tangibly improve your IT infrastructure's resilience against ransomware and other attacks, in addition to presenting a more favorable risk profile to your insurer. Read on to learn MOXFIVE's perspective on where best to begin.

Perspective Rooted in the Trenches

The MOXFIVE team's years of experience responding to threats across a variety of industries and client profiles have taught us much about which technologies and processes most significantly reduce risk. There are some that we feel so strongly about that we recommend implementing them immediately, even if that down-prioritizes other projects within your organization.

Where Should I Start?

The list of security standards and models with which organizations could align can appear daunting. Implementing robust resilience against cyber attacks is a journey, and there are many approaches and tools that can reduce risk effectively. For organizations looking for a place to take the first steps, MOXFIVE recommends applying the risk-based approach as outlined in our Tier 1 measures below.

Tier 1 items provide critical coverage to reduce the risk of the most common types of attacks while easing the response and mitigating the damage should an attacker gain entry. If your organization does not yet have these capabilities, MOXFIVE highly recommends starting towards that goal today.

MOXFIVE is uniquely positioned to help your organization enhance resilience against cyber-attacks with the extensive incident response experience of our Technical Advisors, our partners' hands-on engineering expertise, and our project managers' relentless focus on smooth execution.

2900+

incident response events managed by MOXFIVE Technical Advisors

40%+

average reduction in days to recover using our First 48 Hours playbook

> $300m

saved for cyber attack victims in 2021

Tier 1 Solutions

Endpoint Detection & Response (EDR) with Next Generation Antivirus (NGAV) Functionality: All servers and end-user systems have agents installed and blocking capabilities activated.

- Install tooling on all servers and end-user systems to capture telemetry and block known or suspected malicious activity. This capability can represent the difference between a minor intrusion that can be understood and contained within minutes and a full-blown ransomware attack that materially impacts business.

Multi-factor authentication (MFA): Protect Internet-facing systems including email and VPN.

- Implement MFA for Internet-facing systems so that authentication requires more than just a password. Users often re-use passwords that can be exposed in other attacks and re-used against your systems, and groups with malicious intentions constantly guess common passwords. Make this initial access component of the attack lifecycle harder to succeed.
- Focus on covering email, virtual private networks (VPNs) and other systems that could provide entry to the network. This is critical because without it, Internet-facing systems are one step away from being compromised.

Local Administrator Password Solution (LAPS): Ensure every system has a unique local administrator password that is different from all others.

- This Microsoft tool randomizes built-in “local administrator” accounts’ passwords. We recommend it because it is straightforward to implement, has no additional license cost, and quickly ensures that each and every “local administrator” account has a unique password.
- Implementing LAPS will help thwart an attacker from lateral movement throughout an environment, which is often an inflection point where a simple incident turns into a complex, costly, impactful one.
- We recommend implementing full-featured Privileged Access Management (PAM) once these Tier 1 basics are covered.

Resilient Backups: Isolate archived data from intentional corruption by an attacker who gains access to the network.

- Protect at least one backup mechanism from being corrupted deliberately by an attacker who has administrative-level privileges in the environment. There are multiple approaches to addressing this goal, typically involving a cloud-based secondary backup mechanism.
- Many organizations have designed their backup systems to be resilient against physical disasters such as earthquakes that take a data center offline, but did not design resilience against an attacker intentionally corrupting them. In the age of ransomware, the extortionists continue to refine their tactics to drive forward their business – which is convincing their victims to pay ransom demands. One of the ways they do this is to find and corrupt victims’ backup files – prior to encrypting files – to increase victims’ pain and incentivize them to pay quickly.

System, Patch & Vulnerability Management Tooling: Ensure every system can be managed.

- Install tooling so that IT administrators can take control of any organization-managed system, whether in a physical data center, in a cloud environment, in an office, or in a hotel room with a road-warrior employee.
- Admins must be able to perform basic activities such as installing software, checking for operating system and application vulnerabilities, and installing patches.
- Having this basic capability is crucial to investigating and resolving incidents and has a multitude of other benefits that reduce risk every day.

Understand Internet Footprint: Ensure available services are protected.

- Frequently scan Internet-facing address space to ensure that the systems and services available to the Internet are expected and appropriately protected.
- High-risk services such as Remote Desktop Protocol (RDP), web-based management interfaces, Server Message Block (SMB), Telnet, File Transfer Protocol (FTP), and legacy Simple Network Management Protocol (SNMP) should not be generally accessible to the Internet. Necessary Internet-accessible systems should require multifactor authentication (MFA).
- Assume that services available to the Internet at large will be tested frequently by potential attackers. Frequent scanning helps to ensure that network configurations have not inadvertently exposed systems that were not intended to be Internet-accessible.
- Should higher-risk services be compromised, an attacker may be one step away from dominating the internal network. Make this job more difficult by not presenting such low-hanging fruit.

MOXFIVE is a specialized technical advisory firm founded to help minimize the business impact of cyber attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. With deep roots in incident response and corporate IT, MOXFIVE Technical Advisors strive to be the go-to technical resource for our clients - helping organizations of all types solve their most challenging technology-related problems and provide technical expertise at scale.

www.moxfive.com
(833) 568-6695
info@moxfive.com

MOXFIVE