MOXFIVE

DATA SHEET

Ransomware Readiness

Why is a Ransomware Readiness Assessment Important?

Many organizations find themselves unprepared for a ransomware attack and the specific – and highly effective – techniques that threat actors employ to increase their payout.

This is not a technology problem alone; organizations routinely experience prolonged interruptions due to limited understanding of business-critical IT infrastructure and lack of coordination in their response. MOXFIVE's veteran technical advisors apply a unique perspective that blends technical expertise with a business lens developed through helping thousands of clients respond to ransomware incidents.

Our Approach

The Ransomware Readiness Assessment provides MOXFIVE's assessment of key areas associated with recovering from an attack. MOXFIVE applies our experience with common attack paths and scenarios to lead workshops with a variety of stakeholders across your organization. We cover topics such as infrastructure restoration plans, backup configurations, and team coordination mechanisms that are not typically included in incident response tabletop exercises. This approach is structured to provide rapid value in each workshop to quickly surface the top risks and areas for enhancement.

What to Expect

We have structured our approach to cover the areas most commonly in need of attention. If desired, we can include additional elements – for example, deep dives into particular applications' recovery plans. Our workshop topics include:

- Capability to produce a prioritized list of applications and their associated infrastructure to drive recovery efforts
- Processes for emergency implementation of server, end-user, network, and backup system containment measures
- Backup tooling and configurations, tamper-proofing against attackers who gain internal network access, restoration times
- Active Directory and network architecture
- Coordination processes to execute scenarios such as validating backups, restoring servers, building new servers, installing and validating application functionality, and helpdesk support while under time pressure

Benefits of working with MOXFIVE

IT & Security Expertise On-Demand

With a deep understanding of both IT operations and security, MOXFIVE Technical Advisors can provide the expertise you need and help determine the most efficient and cost-effective solution.

Access to Experts at Scale

MOXFIVE maintains an ecosystem of the industry's best technology experts and service providers so we can quickly assemble the right team with the skills you need.

Streamlined Process

MOXFIVE manages the selection, implementation and procurement processes to keep projects on schedule and minimize disruption.

Resilient Outcomes

MOXFIVE identifies gaps between business, IT and security objectives to build a more resilient environment.

Sample Schedule:

Week 1: Project kick-off, documentation review, and preparation

Week 2: Workshops on pre-incident preparation measures including the Identification and Orchestration process.

Week 3: Begin workshops on post-incident measures starting with Initial Containment Measures

Week 4: Post-incident workshops on Eradication and Deep Dive Investigation

Week 5: Workshop on Surge Infrastructure and Services

Week 6: Workshop on Recovery

Weeks 7 - 8: Deliver final observations & recommendations presentation

As we facilitate the workshops with your team, we use scenarios like the following to guide discussions based on our ransomware response experience:

- A significant ransomware attack has occurred, and the availability and viability of backups is not yet known.
- Some confirmed indications of a ransomware attack have been detected, but the extent of the intrusion and ransomware deployment have not yet been confirmed.
- Ransomware impact is confirmed and is limited to servers within a particular geographic region, cloud environment, or data center.
- Server infrastructure managed by an outsourced service provider is impacted by ransomware.
- Ransomware attack affects authentication for a significant number of users (i.e., based on impacts to Active Directory servers).
- Ransomware attack affects a significant number of end-user workstations/laptops in a region.
- Organization obtains a decryption tool from the threat actor and wants to proceed to decrypt servers.

Enhancing Capabilities

Post-assessment, MOXFIVE can assist with implementing processes and technologies such as the below to bolster your response capabilities.

- Tabletop exercises to test processes with real-world scenarios
- Red Team / Purple Team engagements to test technical prevention, detection, and response controls
- Playbook development, including general recovery processes, and detailed per-application recovery plans for the most business critical infrastructure
- Implementation of automation tooling to enhance the internal SOC's efficiency and effectiveness
- Security awareness training and phishing simulations
- Technology procurement and implementation (e.g., EDR, MFA, PAM, backup solutions)

MOXFIVE is a cybersecurity company helping organizations respond to incidents and minimize the risk of future 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. Through a combination of our technical experts and proprietary platform, we bring order to chaos and deliver a tailored incident response approach and resilience-minded path forward for clients of all sizes, faster and more efficiently. .

🌐 www.moxfive.com

☎ (833) 568-6695

✉ info@moxfive.com

MOXFIVE