Ransomware Preparedness Services

Ransomware represents a significant threat for most organizations, and the frequency and financial impacts of these potentially devastating attacks continue to escalate.

In response to the rise in attacks, cyber insurance providers are raising the bar for the level of preparedness their clients must achieve to qualify for payouts and policy renewals.

Facing Down A Major Corporate Risk

Recent statistics highlight the severity of the ransomware problem and the potential financial impacts on organizations.

> In 2021, the **largest ransomware payout** was made by an insurance company at **$40 million,** setting a world record.[1]
>
> The average **cost to recover** from a ransomware attack is **$1.85 million.**[2]
>
> 66% of survey respondents reported their organization suffered **significant revenue loss** as a direct result of a ransomware attack, and 53% reported that their brand suffered.[3]
>
> 1. Insurance Journal, 2021; 2. Sophos, 2021; 3. Cybereason, 2021

The good news is that Tevora's proven ransomware preparedness services can help you improve and practice response techniques, ensuring you are ready to respond effectively to minimize the potential impacts of these insidious attacks.

Ransomware Preparedness

Services

Ransomware **Threat** Assessment

A threat-based assessment to identify, validate, and provide remediation steps for any vulnerabilities that can be exploited for potential ransomware attacks.

Utilizing a Purple Teaming approach in which our Red Team partners with your Blue Team to identify and validate ransomware attack vectors.

Simulating real world ransomware attacks by using the latest ransomware payloads and attack strategies, as well as our Threat team's deep knowledge base and expertise to help you be better prepared.

Ransomware **Readiness** Assessment

Using tabletop attack scenarios and exercises to ensure your people, processes, controls, and technologies are up to date and ready to handle any adverse scenario.

Evaluates your ability to effectively and quickly respond to a ransomware attack.

Identifies weak points in your systems to dramatically reduce your attack surface.

Enterprise Ransomware **Risk** Assessment

Bringing together key stakeholders to identify and assess potential threats, prioritize and implement key security controls, and treat any ransomware-related risks that pose a threat to your organization's strategy and objectives.

What Are the Benefits of Using Tevora's Ransomware Preparedness Services?

Expertise and Experience. Tevora's cyber security professionals have worked with many of the world's leading companies to help prepare them for potential ransomware attacks with various tools, policies, and procedures in place to ensure an effective and quick response should an attack occur. Our experienced team is able to leverage the learnings from these engagements to help ensure you are ready if an attack occurs.

Fortified Defenses. Ultimately, Tevora's ransomware preparedness services are focused on strengthening your defenses against ransomware attacks. They ensure your team and environment are ready to respond quickly and efficiently to mitigate or entirely avoid the impacts of ransomware attacks.

Compliance With Cyber Insurance Requirements. Tevora helps you meet your cyber insurance provider's requirements to ensure the maximum possible payout in the event of a ransomware attack. This also ensures you will be eligible for renewal when your current policy expires.

ACHIEVED ACCREDITATIONS:

AUTHORIZED ASSESSOR:

PCI DSS QSA
PCI PA-DSS QSA
3DS ASSESSOR
PCI FORENSIC INVESTIGATOR

Tevora is a specialized management consultancy focused on cyber security, risk, and compliance services. Our combination of collaborative strategic planning and skillful execution make us a trusted partner to some of the most famous brands in the world.

Go forward. **We've got your back.**

Privacy Impact Assessment

Assesses privacy risks and considerations related to the data in your environment and the security controls in place to protect it.

Focuses on the types of processing operations that are likely to result in a high risk to the privacy rights of the people whose personal information you are handling.

Helps you understand how your sensitive data is used and how it may be exposed to ransomware attacks.

Data Mapping Service

Provides a detailed map of how your data is used, where it comes from, how it flows through your organization, and who it is shared with.

Uses data visualization capabilities to graphically depict the flow of data through your organization.

Provides documentation of data usage and flows that can be helpful for making decisions on data usage and protective measures.

Helps you identify what data may be exposed to ransomware attacks.