IBM Cyber Rapid Risk Readiness Assessment

Bring stability to a complex IT environment

Business benefits

- Identifies risk in your IT and service delivery environment
- Produces a failure mode and effect analysis on your main service components
- Prioritizes remediation and mitigation activities based on value at risk and probability of occurrence

Cyber incidents are increasing in sophistication and intensity. When these attacks happen, some of the costlier consequences are data loss, inaccessibility, failure of public or client applications and websites. Companies are experiencing larger and more frequent data breaches as a result of malicious or criminal cyber-attacks. According to a recent Ponemon Institute study sponsored by IBM, the average cost of a data breach is USD3.6M.[1] The material disruptions caused by data breaches can have extensive effects on customers, investors and employees who have a stake in a service or application's availability and consistency. No government agency or business can tolerate the downtime from cyber attacks such as ransomware or malware without negative effects.

If you have experienced a cyber incident or you are concerned about your preparedness for potential cyberattacks, IBM® Cyber Rapid Risk Readiness Assessment can assist in bringing stability to your environment and providing you with a roadmap to a more robust and predictable resiliency capability.

Highlights

- Assess whether resources are deployed or invested optimally to help better manage cyber risks
- Determine a roadmap of recommended remediation over a proposed timeframe in journey towards desired state
- Identify issues and exposures to downtime caused by cyber attacks
- Establish a baseline of existing cyber resiliency response posture for further consideration and action to help you manage risks and prepare for contingencies against possible future threats and failures

The Challenge

Many organizations are behind the curve in terms of cyber-resiliency acumen, relying mainly on stationary self-protective measures and compliance-oriented processes. Moving to a "cyber-resiliency" oriented position is demanding, and transformation needs to occur across the harmony of people, processes and technologies. Some of the concerns during such a transition may include:

- Is our cyber-resiliency strategy aligned with our business objectives?
- How do we measure the effectiveness of our cyber-resiliency program?
- Would we know if we were the victim of a breach?
- Do we have the right resources, initiatives, processes, technologies and investments to protect, respond and recover from a cyber-attack?
- Can we adequately be protected from new and emerging threats?
- Can we proactively respond to changes in the business and regulatory environment?
- Do we have the right strategy to respond swiftly to a cyber-attack?

The Offering

IBM Cyber Rapid Risk Readiness Assessment provides an in-depth review of existing processes, people and technology in order to determine preparedness against cyber-attacks and enable clients to understand areas of vulnerability, pain points and concerns. With a flexible scoping model, IBM works with you to identify the areas to address, processes to include within that scope and the infrastructure layers (facilities, server, storage, networks, database, application) to review. IBM can then focus on those scope areas and deliver a report on what risks may exist within each of the layers and processes that support your business, the potential impact of those risks and the likelihood of those risks materializing. IBM can also include in the report a prioritized list of recommendations to help remediate the risks with higher impact.

Offering Scope

Understand and assess the following areas:

- Business Continuity—existing process, documentation maturity, planning framework and execution mechanisms
- Incident Management procedures
- Backup Strategy
- Network Maintenance
- Security Configurations, Compliance to industry frameworks, Security Incident response plans etc.

Offering Value Proposition

Providing impact information to justify your IT resiliency investments

This analysis can provide you with a wealth of crucial information, including the essential processes that support your services and infrastructure (cloud, traditional or a combination of both); the cost; and probability of disruption and data loss. It also reports the actual achievable recovery time and recovery point objectives should a cyber incident occur.

Helping you select the right strategy for your business

By providing a robust analysis of impact on your business, IBM Cyber Rapid Risk Readiness Assessment helps you define, develop and implement the correct remediation for your organization. The mitigation strategies are based on a thorough understanding of the unique availability, recovery and resiliency requirements that your services possess.

Why IBM?

IBM's approach to making your business more resilient is designed to be end to end—covering strategy and vision, organization and human resources, business processes, applications, data, and technologies and facilities. With over 50 years of experience helping businesses improve their resilience, IBM is a leader in addressing business, data and event-driven risks. IBM provides highly skilled resiliency expertise to help you assess, design, implement, test and sustain a sound enterprise business-based resiliency program.

For more information

To learn more about IBM Cyber Rapid Risk Readiness Assessment, please contact your IBM sales representative or visit the following website:

Resiliency Consulting Services

IBM Resiliency Services
3039 Cornwallis Rd., Bldg. 201
Research Triangle Park, NC 27709

Produced in the United States of America
September 2017

[1] Ponemon Institute. "2017 Cost of Data Breach Study." June 2017. www.ibm.com/services/us/en/it-services/business-continuity/impact-of-business-continuity-management/index.html

Please Recycle

BUJ03175-USEN-00