LRS
LEVI, RAY & SHOUP, INC.

Shifting Paradigms

From Data Protection to Data Resilience

INTRODUCTION

Digital Landscape

The digital landscape is constantly evolving, and with it, so must your approach to data security. The estimated global cost of cybercrime is expected to surge from $9.22 trillion in 2024 to an astounding $13.82 trillion by 2028.[1]

The stakes for data security have never been higher. From sophisticated cyber threats and an increasing attack surface to increasingly complex regulatory requirements, you face an intricate web of new challenges in safeguarding your valuable data assets. Recent high-profile data breaches and cyberattacks serve as stark reminders of the potential consequences of inadequate security measures. As such, a new approach to cybersecurity is required—one that prioritizes data resilience.

Building on the foundation laid by traditional data protection strategies, data resilience offers additional layers of protection and recovery to create a dynamic security posture. In this paper, we will explore the crucial role data resilience plays in creating an agile and secure operational environment, with best practices to get you started.

FROM DATA PROTECTION TO DATA RESILIENCE: A NECESSARY EVOLUTION

Traditional security systems that focus on data protection are vital in safeguarding systems against intrusion and ensuring data remains inaccessible to unauthorized users. However, as threats become more sophisticated, newer, more adaptive measures are required. Data resilience builds on data protection to offer a more comprehensive security strategy. Beyond preventative measures, data resilience adds an element of preparedness to ensure you're poised to respond and recover efficiently should an incident occur.

"[It's] no longer a matter of 'if' but 'when' an organization will suffer a data breach," says internationally recognized IT security expert, author, and speaker Torsten George. "This means that instead of primarily focusing efforts on keeping threat actors out of the network, it's equally important to develop a strategy to reduce the impact," he adds.[2]

> *"[It's] no longer a matter of 'if' but 'when' an organization will suffer a data breach. This means that instead of primarily focusing efforts on keeping threat actors out of the network, it's equally important to develop a strategy to reduce the impact."*

Data Resilience

Adopting a data resilience cybersecurity approach is more than a defense tactic; it's a strategic imperative that secures the future of your enterprise, and here's why:

- **ENSURES BUSINESS CONTINUITY:** A network outage caused by a cyberattack or any other unexpected event, can lead to devastating loss that could bring your business to a complete halt. In fact, the average cost of downtime is $1,467 per minute—or $88,020 per hour.[4] Data resilience prioritizes rapid recovery and operational continuity in the face of these events, minimizing downtime to preserve productivity and revenue streams.
- **SIMPLIFIES REGULATORY COMPLIANCE PROCESSES:** As regulatory scrutiny intensifies, you must be able to adapt to and meet the demands of changing regulations. Because data resilience encompasses broader compliance features than traditional data protection tools, such as automated data retention policies, audit trails, and encryption controls, you can more easily maintain adherence to complex regulations.
- **INSTILLS TRUST AND PROTECTS YOUR REPUTATION:** Beyond the massive financial implications, data breaches can also erode customer trust and tarnish your brand's reputation. According to research of 4000 consumers across the globe, 81% say they would stop engaging with a brand online following a data breach.[3] By establishing robust mechanisms for rapid response and recovery, you can quickly restore operations and secure customer data to maintain trust and mitigate any damage to your brand's reputation in the aftermath of a breach.

Data resilience is not just the latest buzzword; it's being widely recognized as an essential cyber-security strategy for businesses across the globe. In fact, leading analyst firms like Gartner are advising businesses to transition from traditional cyber defenses to a resilience-based approach, focusing on managing disruption to minimize the impact of cybersecurity incidents.[4]

Data Resilience is a Game-Changer

Powers informed decision-making: Data resilience practices are grounded in real-time data and advanced analytics, arming you with the information you need to quickly grasp the ramifications of an incident and take decisive action. This data-driven approach allows you to steer your organization more effectively through crises and adapt to threats with foresight.

Bolsters innovation and agility: Protecting your critical data is about more than just preventing loss and maintaining operations; it also provides a stable foundation for innovation and agility. Secure, readily available data fuels analytics that inspire breakthroughs, drive strategic decisions, inform new business models, and nimbly respond to market trends, so you can maintain your competitive edge.

Cost savings: Integrating AI-powered threat detection and automation within data resilience frameworks not only bolsters real-time threat detection and response, but also streamlines and accelerates the post-breach recovery process to keep costs down. According to IBM's Cost of a Data Breach Report 2023, organizations that have fully deployed security AI and automation technologies have saved an average of $1.76 million in the event of a data breach compared to those without such measures.[6]

Five Steps to Adopting Data Resilience

Moving from data protection to data resilience requires a fundamental shift in mindset, strategy, and execution. Here are five best practices to guide this transition:

1. **Perform ongoing risk assessments:** Regularly evaluate and identify the most critical data and systems, potential threats, and vulnerabilities to get a clear understanding of where resilience needs to be bolstered. Complete thorough risk assessments that go beyond traditional perimeter defenses to include internal and external threats, as well as emerging risks such as supply chain vulnerabilities and third-party dependencies. By continuously monitoring the threat landscape and assessing your organization's risk exposure, you can stay one step ahead of potential threats and proactively mitigate risks before they escalate.

2. **Develop a comprehensive resilience strategy:** Create a detailed plan that goes beyond data protection to encompass a holistic resilience strategy. Integrate encryption, access controls, and threat detection with robust backup and recovery mechanisms, clear disaster recovery and incident response protocols, and seamless business continuity processes. By weaving together these critical components, you can establish a resilient framework that safeguards data integrity, protects against unauthorized access, and ensures rapid recovery and continuity of operations in the face of disruptions.

3. **Establish robust data redundancy and backup procedures:** Ensure the safety of critical data by instituting comprehensive redundancy systems and backup protocols. Store crucial datasets in secure, diversified locations, encompassing both on-site and cloud-based environments. Regularly test and validate backups to ensure their effectiveness in restoring data integrity and functionality in the event of a disruption.

4. **Invest in training and awareness:** Educate employees on their role in data security, risks, and response procedures with comprehensive training on cybersecurity best practices. By leveraging tools that offer visibility and insights into storage security threats and best practices, you can support these efforts with enhanced awareness and proactive measures to safeguard critical data assets.

5. **Adopt a continuous improvement approach:** Continually refresh and rigorously test your resilience plans to address emerging threats and incorporate the most current data protection and recovery technologies. Employ advanced security features, such as encryption, access controls, and threat detection, to proactively defend against and stay ahead of evolving cyber threats. This proactive stance not only protects data integrity but also continuously strengthens your cyber defenses.

Cyber Threats are Evolving and So Must Your Response to Them

Your Ability to Recover

While preventing destructive events from occurring is critical, equally as important is your ability to recover when—not if—the inevitable happens.

LRS can help. For over 25 years, we've served a diverse range of clients, from enterprise accounts to mid-market and public sectors. Our team has been at the forefront of innovation, orchestrating the modernization and automation of workloads across industries, both on-premises and in the cloud. With a cadre of experts in Data, Analytics, and AI, led by industry veterans with over two decades of experience, we can help you unravel even the most intricate business challenges.

Meanwhile, our Security Practice, helmed by former CIOs and CISOs with extensive backgrounds in critical sectors like government and manufacturing, empowers clients to navigate the complex landscape of data security and compliance with ease.

As an IBM Platinum partner, LRS can fortify your data resilience strategy with premier solutions that not only enhance data security and orchestrate seamless operations.

ABOUT LRS

LRS offers comprehensive technology solutions encompassing servers, storage, software, and services that help businesses reduce costs, increase revenue, and minimize risk. Founded in 1979, LRS is known for building solutions that consistently deliver insights, fuel operational efficiencies, and close critical vulnerabilities, with the ability to scale capacity and upgrade service to meet current and future data needs.

IBM Platinum Partner

1 https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
2, 4 https://www.securityweek.com/cyber-resilience-new-strategy-cope-increased-threats/
3 https://hub.pingidentity.com/survey/3464-2019-consumer-survey
5 https://www.comparitech.com/data-recovery-software/disaster-recovery-data-loss-statistics/
6 https://www.ibm.com/reports/data-breach