Emerge Stronger with Cyberus Systems' Disaster Recovery Prevention (DRP)

Cyberus Systems ZTSaaS:

Reinforcing Disaster Recovery Protection (DRP) in the Zero Trust Era

In today's interconnected digital world, the significance of Disaster Recovery (DRP) within the Zero Trust Security model cannot be overstated. **Cyberus Systems' Zero Trust Security as a Service (ZTSaaS)** provides a holistic DRP strategy intricately woven into your organization's cybersecurity practices.

Here are some pertinent cybersecurity attack and breach statistics specifically related to Disaster Recovery:

1. **Prevalence of Cyber Attacks Leading to Disasters**: A significant percentage of businesses experience cyberattacks that result in the need for disaster recovery efforts. For instance, a survey by CyberEdge Group found that over **80%** of organizations were affected by a successful cyberattack.
2. **Ransomware and Disaster Recovery**: Ransomware attacks have been a major driver for disaster recovery plans. According to Verizon's 2021 Data Breach Investigations Report, ransomware attacks accounted for **10%** of the breaches, an increase from the previous year, highlighting the critical need for effective disaster recovery strategies.
3. **Cost of Downtime**: Downtime due to cyber incidents is a critical concern for businesses. A report by Datto Inc. found that the average cost of downtime for small to medium-sized businesses was approximately $141,000 in 2020, a significant increase from $46,800 in 2019.
4. **Time to Recovery**: Recovering from a cyber incident can be lengthy. On average, it takes companies approximately 21 days to fully recover from a ransomware attack, according to Coveware.
5. **Lack of Preparedness**: Despite the increasing risk, many organizations are still unprepared for disaster recovery. A

study by the Ponemon Institute reported that only 27% of companies have a comprehensive disaster recovery plan in place.

6. **Data Loss Statistics**: Data loss is a common consequence of cyberattacks, with significant percentages of businesses experiencing data loss due to these incidents. For example, the World Backup Day survey indicated that 30% of people have never backed up their data.
7. **Cloud-Based Disaster Recovery**: The adoption of cloud-based disaster recovery solutions is rising due to their cost-effectiveness and efficiency. An Enterprise Strategy Group (ESG) survey found that 40% of organizations use the cloud as part of their disaster recovery strategy.
8. **Impact of COVID-19**: The COVID-19 pandemic has increased cyber threats and highlighted the importance of robust disaster recovery plans. The shift to remote work has particularly exposed vulnerabilities in many organizations' disaster recovery plans.
9. **Recovery Point Objective (RPO) and Recovery Time Objective (RTO)**: Achieving aggressive RPOs and RTOs is challenging for many organizations. According to a report by Zerto, 91% of businesses have an RPO and RTO of less than one hour, but only 10% can achieve this goal in practice.
10. **Business Continuity Challenges**: Maintaining business continuity in the face of cyber incidents remains challenging, with many businesses struggling to integrate their disaster recovery and business continuity plans effectively.

These statistics underscore the importance of incorporating robust disaster recovery measures within the broader context of cybersecurity strategies. Regularly updating and testing disaster recovery plans, backing up data, and educating employees on best practices are crucial to enhancing an organization's resilience against cyber threats.

Here are some key statistics, facts, future predictions, and projections you should know related to Disaster Recovery in the context of cybersecurity:

1. **Rising Incidence of Cyberattacks Requiring Disaster Recovery**: With the increasing frequency and sophistication of cyberattacks, particularly ransomware, robust disaster recovery solutions have become more critical. Statistics show that many businesses experience cyberattacks that lead to substantial data loss and downtime.
2. **Cost of Downtime and Data Loss**: The financial impact of downtime due to cyber incidents is significant. Reports indicate that the average cost of downtime for businesses can run into hundreds of thousands of dollars, emphasizing the importance of efficient disaster recovery planning.
3. **Ransomware and Its Impact**: Ransomware attacks are a major driver of disaster recovery efforts. The proliferation of ransomware has forced many organizations to revisit and strengthen their disaster recovery strategies.
4. **Recovery Time Objectives (RTOs)**: Achieving quick recovery times is a major business challenge. The industry standard for RTOs is becoming increasingly stringent, with many organizations aiming for recovery times of a few minutes to an hour.
5. **Cloud-Based Disaster Recovery Solutions**: The adoption of cloud-based disaster recovery solutions is growing due to their cost-effectiveness, scalability, and efficiency. Future trends

indicate a continued shift towards cloud-based disaster recovery strategies.

6. **Lack of Preparedness**: Despite the growing threat landscape, many organizations remain underprepared for effective disaster recovery. Studies show that many businesses do not have a comprehensive disaster recovery plan.
7. **Impact of Remote Work**: The shift to remote work has introduced new complexities in disaster recovery planning. The decentralized nature of remote work environments requires more robust and flexible disaster recovery solutions.
8. **Automation in Disaster Recovery**: There is a growing trend towards automating disaster recovery processes. Automation helps reduce recovery time and minimizes the chances of human error during recovery.
9. **Integration with Cybersecurity Measures**: Future disaster recovery planning is expected to be more tightly integrated with overall cybersecurity strategies. This integration includes proactive threat monitoring and automated responses to potential threats.
10. **Investment in Disaster Recovery**: Businesses are expected to increase their investment in disaster recovery solutions, recognizing the high costs associated with cyber incidents and the importance of maintaining business continuity.
11. **Regular Testing and Updates**: There is an increasing emphasis on regular testing and updating disaster recovery plans to ensure they remain effective against evolving cyber threats.

The Imperative of Disaster Recovery in Zero Trust

Disaster Recovery is crucial in the Zero Trust model because it ensures the organization can recover quickly and efficiently even when a security breach occurs. In a zero-trust framework, DRP is not just about restoring data and systems; it's about fixing them to maintain the ongoing trust and integrity of the entire network.

Impact of Cyberus Systems' on Security Posture

- ***Enhanced Resilience:*** Robust DRP capabilities mean businesses can withstand and quickly recover from cyber incidents, minimizing operational and financial impacts.
- ***Maintains Customer Trust:*** Quick and effective disaster recovery maintains customer confidence by demonstrating reliability and security commitment.
- ***Regulatory Compliance:*** Effective DRP strategies ensure compliance with various data protection regulations, often mandating specific recovery capabilities.

Cyberus Systems' ZTSaaS DRP Solutions

"Be proactive, not reactive, in cybersecurity. Choose Cyberus Systems ZTSaaS for advanced DRP on your journey to Zero Trust.

Take the Next Step in Advanced DRP with Cyberus Systems' ZTSaaS"

Leveraging the CISA Zero Trust Maturity Model, our ZTSaaS services are categorized into Traditional, Advanced, and Optimal solutions, ensuring that every organization can find the right level of security to meet their needs:

Traditional:

- ***Basic DRP Services:*** Ensures fundamental recovery capabilities, focusing on rapid data and system restoration.
- ***Regular Data Backups:*** Frequent and reliable backups to ensure data is always recoverable.

Advanced:

- ***Expert Analysis and Planning:*** In-depth risk assessments and business impact analyses to tailor a DRP plan to your organization's specific needs.
- ***Rapid Response Protocols:*** Quick activation of response plans to minimize downtime and restore functionality.

Optimal:

- ***Zero Trust Integration:*** DRP solutions fully integrate within a Zero Trust framework, ensuring secure and verified recovery steps.
- ***Future-Proof Strategies:*** Adaptable DRP plans that are prepared for evolving cyber threats and technological advancements.
- ***Continuous Improvement:*** Post-recovery analysis to strengthen defenses and enhance resilience against future incidents.

Importance of Cyberus Systems DRP Services

- ***Increasing Cyber Incidents:*** Studies show that cyber incidents have increased in frequency and severity, making effective DRP more crucial than ever.
- ***Cost of Downtime:*** The average cost of IT downtime is estimated at thousands of dollars per minute, highlighting the financial imperative of rapid recovery.
- ***Recovery Challenges:*** Over 40% of businesses that experience a disaster never reopen, and 25% of those that do reopen close within two years, underscoring the need for robust DRP planning.

Choose Cyberus Systems ZTSaaS for Superior DRP

With Cyberus Systems ZTSaaS, you're not just preparing for potential disasters but equipping your business to emerge stronger and smarter from them. Our comprehensive DRP solutions ensure that your business is always ready to face and overcome the challenges of the digital era.

Build a Resilient Future with Cyberus Systems ZTSaaS

Don't leave your organization's future to chance. Partner with Cyberus Systems and transform disaster recovery from a reactive process into a proactive strategy. Prepare for the worst and perform your best with Cyberus Systems ZTSaaS.

"With Cyberus Systems ZTSaaS, bounce back faster, stronger, and smarter."

Are you ready to reinforce your organization's digital defense? It's time to take

action. Cyberus Systems invites you to elevate your cybersecurity posture with our state-of-the-art Zero Trust Security as a Service.

Step beyond the limitations of traditional defense in depth and safeguard your enterprise with our holistic, Zero Trust approach.

Embrace a future where every identity is meticulously validated, every access is scrutinized, and every user interaction is an opportunity to fortify your security.

Initiate Your Zero Trust Security Transformation

Unlock the full potential of cutting-edge identity protection. Begin your journey with a comprehensive Zero Trust Security Assessment from Cyberus Systems.

Our expert team guides you through a detailed evaluation of your security measures, identifies potential vulnerabilities, and provides tailored recommendations to enhance your defenses.

Cyberus Systems Zero Trust Security Assessment Today

Contact us to schedule your Zero Trust Security Assessment: https://cyberussystems/aspirin/. Let us demonstrate how our ZTSaaS solutions can align with your unique needs, ensuring compliance with the most stringent regulatory and industry standards. Choose Cyberus Systems and commit to advanced, proactive security.

Your Next Steps:

1. ***Please schedule a Consultation:*** Reach out to our team and schedule a time to discuss your organization's security needs.
2. ***Zero Trust Security Assessment:*** Allow us to conduct a thorough assessment and tailor a strategy that fits your organization's profile.
3. ***Customize Your ZTSaaS Plan:*** Based on the assessment, we'll help you choose the mix of Traditional and Optimal services that align with your security maturity and business objectives.
4. ***Implement and Thrive:*** With our ongoing support, watch your organization's security transform, building resilience against tomorrow's threats.

Your organization's identity security is paramount. Let Cyberus Systems be your ally in building a zero-trust environment.

"Secure your future with Cyberus Systems — where trust is earned, and security is absolute.

With Cyberus Systems ZTSaaS, bounce back faster, stronger, and smarter. Reach out now to fortify your disaster recovery strategy."

Provided as an Educational Service By:
Cyberus Systems LLC
Safeguard Your SMB with CyberUS!
173 Saint Patrick DRP. Ste 104 #144
Waldorf, MD 20603
Main: 888-808-1830
Email: Support@Cyberussystem.com
https://Cyberussystems.com/contact-us