RESILIENCE

Disaster Planning for Banking: Your Cyberattack Recovery Guide

Natural disasters can wreak havoc on business operations with power outages and property damage; but there are other types of disaster recovery scenarios Financial Services (or FinServ) organizations need to plan for to protect critical assets. We're talking about cyberattacks. The cyberthreat landscape is more dangerous and sophisticated than ever. Banking organizations can be attractive targets for cybercriminals and must be prepared to stand against these threats both from a cybersecurity and risk management standpoint, and a team member training perspective. So, how can you determine if your FinServ organization is ready for the unthinkable?

Disaster readiness means more than conducting basic risk assessments. It also means creating a detailed, well-developed, and tested disaster recovery plan. You don't want to wait until disaster strikes, scrambling to figure out next steps when connectivity is lost or what to do if your systems are crippled. Planning ahead is critical to both prevention and successful cyberattack recovery. That's why UDT has partnered with Locality Bank to bring you this expert guide for establishing business continuity in the event of a cyberattack—the key to providing the essential services your customers and community relies upon, no matter what.

Why Develop Your Disaster Recovery Plan (DRP)?

A robust disaster recovery strategy is required for any Financial Services organization to maintain information security against potential threats. This plan ensures that, in the event of a cyberattack, your organization can quickly recover and continue to operate. Without a cyber-specific incident response plan, the consequences of a cyberattack can be catastrophic, leading to prolonged downtime, loss of customer trust, and severe financial repercussions.

Back in February 2024, we offered our readers a Comprehensive Checklist for Disaster

Back in February 2024, we offered our readers a Comprehensive Checklist for Disaster Recovery Planning intended to offer a starting point for recovery from a disaster or data breach event. Considering the current turbulent climate, however, we want to revisit this topic and offer a far more detailed set of planning guidance. We also recommend designating a few employees and/or stakeholders as your organization's disaster recovery team.

How Cyberthreat Landscape Impacts Customer Confidence

Cyberthreats are evolving at an unprecedented rate. From ransomware attacks to sophisticated phishing schemes, the tactics used by cybercriminals are becoming more advanced. A successful cyberattack and/or data breach can lead to significant financial losses, regulatory penalties, and reputational damage, the latter of which is most impactful on your customer relationships. When it comes to reputational damage, how a business reacts after a breach can have a major difference in the perception of a banking institution—positive or negative.

It's important to note that while no organization is immune to cyberthreats, developing a disaster recovery plan for your organization can prevent cyberattacks from paralyzing operations and getting away with sensitive data in a security incident, all damaging contributors to customer trust. Financial Services organizations can differentiate themselves by earning the confidence of the communities they serve by demonstrating excellent physical and digital security posture, a zero-risk approach, and attentive, validated, and regularly tested disaster recovery planning.

The "4R" Method for Disaster Recovery

To create an effective disaster recovery plan, Financial Services organizations should consider the "4R" method: Recovery Time Objective (RTO), Recovery Point Objective (RPO), Data Replication, and Recurring Testing.

- **Recovery Time Objective (RTO)**:
  - **Definition**: RTO is the maximum acceptable amount of time that your organization can be offline after a disaster or cyberattack before normal operations must be resumed.
  - **Importance**: Establishing a clear RTO helps prioritize recovery efforts and allocate resources effectively. For Financial Services, minimizing downtime is crucial to maintaining customer trust and regulatory compliance.
- **Recovery Point Objective (RPO)**:
  - **Definition**: RPO is the maximum acceptable amount of data loss measured in time. It determines how much data your organization can afford to lose in the event of a disaster or cyberattack.
  - **Importance**: Setting an appropriate RPO ensures that critical data is backed up frequently enough to prevent significant loss. In the Financial Services sector, where data accuracy is paramount, a low RPO is essential and data backup a requirement.
- **Data Replication**:
  - **Definition**: Data replication involves copying data from one location to another to ensure that a backup is available in case of a disaster.
  - **Importance**: Implementing data replication strategies, such as real-time replication or periodic backups, ensures that your organization can quickly restore data and resume operations. This is particularly important for Financial Services organizations that handle large volumes of transactions and sensitive information.
- **Recurring Testing**:
  - **Definition**: Recurring testing involves regularly testing your disaster recovery plan to ensure that it works as intended.
  - **Importance**: Regular testing helps identify potential weaknesses in your

disaster recovery plan and allows for continuous improvement. For Financial Services organizations, recurring testing is vital to ensure that recovery procedures are up-to-date and effective in the face of evolving cyber threats.

Potential Disaster Scenarios

To effectively prepare for cyberthreats, Financial Services organizations must examine potential disaster scenarios. Some common scenarios include:

- **Malware & Ransomware Attacks**: Cybercriminals encrypt your organization's data and demand a ransom for its release. Without a robust disaster recovery plan, your organization may be forced to pay the ransom or face prolonged downtime.
- **Phishing Schemes**: Employees are tricked into providing sensitive information or clicking on malicious links, leading to data breaches. A disaster recovery plan ensures that your organization can quickly respond to and mitigate the impact of such breaches.
- **Distributed Denial of Service (DDoS) Attacks**: Cybercriminals overwhelm your organization's servers with traffic, causing them to crash. A disaster recovery plan helps ensure that your organization can quickly restore services and minimize downtime.

Steps to Create a Cyberattack Recovery Plan

Use the following steps to map out your organization's cyberattack business continuity plan:

1. **Assess Risks**: Identify potential cyberthreats and assess their impact on your organization.
2. **Define Objectives**: Establish clear RTO and RPO targets based on your organization's needs.
3. **Implement Data Replication**: Set up data replication strategies to ensure that backups of critical systems are available in an offsite data center or with cloud services.
4. **Develop Procedures**: Create detailed procedures for responding to different types of cyber threats.
5. **Test Regularly**: Conduct recurring tests to ensure that your disaster recovery plan is effective against disruptive events or equipment failures due to a cyberattack. This includes validating your backups and doing 3-4 partial restore tests each month to ensure your data can be recovered in the required time. Your organization should also do an annual full-restore test to confirm all procedures are up to date and working as designed.
6. **Review and Update**: Continuously review and update your disaster recovery plan to address new threats and changes in your organization.

Ensure Business Continuity After a Cyberattack

The cyberthreat landscape is constantly evolving, and Financial Services organizations must be prepared to stand against potential IT disasters. By understanding potential disaster scenarios and implementing the "4R" method, your organization can create a robust disaster recovery plan that ensures business continuity and protects the communities relying on your services. Don't wait until disaster strikes—take action now to safeguard your organization's IT systems in the future.

What's Your Security Risk Level?

Take UDT's brief cybersecurity quiz to assess your organization's risk and get tips on improving it.

Locality Bank, based in Fort Lauderdale, FL, is dedicated to empowering local

businesses to maximize their potential—including providing the resources and knowledge to protect against risks like cyber threats. For additional insights and guidance, visit Locality's Resource Center at www.localitybank.com/resources.

Contact UDT today to find out how we can help make sure your organization has the technology and services it needs to keep data secured against human error and cyberattacks, and that you are prepared for whatever disaster might attempt to take down your IT infrastructure. Stay safe with a service provider you can trust.