9 Steps to Mitigate Risk from Cyber Threats

Assess and strengthen your preventative & restorative data security strategies

An Unprecedented Threat Landscape

Companies and firms now face more pervasive threats than ever before, as cybercriminals have become more sophisticated in targeting industries with sensitive data to make a quick buck, steal information or disrupt operations.

Given that cybersecurity incidents have evolved from "if" to "when" and "now" to "again", the downtime that results from a breach now has similar impacts on reputation and the bottom line as natural disasters or prolonged power outages do. For this reason, IT departments must integrate their cybersecurity and IT disaster recovery (DR) programs together into a single response plan. But where do you begin?

The 2-Pronged Approach to Data Security

Preventive measures are key to securing your organization's systems. But failure to establish a restorative strategy is a missed opportunity. To effectively mitigate IT risk, organizations must embrace a two-pronged approach of both preventative and restorative measures, giving the two equal attention.

Preventative: Stops a technology disruption or attack from happening
Restorative: Recovers from any technology disruption or attack that does occur

This dual emphasis contributes to a holistic resiliency strategy for your entire organization, covering both sides of the threat equation. As a bridge between these two areas of prevention and restoration, organizations should also adopt a means of detection to identify when a breach or disruption has occurred, in order to execute a restorative plan.

1. Preventative
Threat Management
Access Control
Endpoint Protection

Detection
Bridge Strategies
with Detection
Process

2. Restorative
Archiving
Backups
Replication

Restorative Strategies Often Go Neglected

A Bluelock-IDG survey of IT managers and executives examining the state of IT security practices found that over half (59%) of respondents prioritize prevention over restorative measures. Yet, when asked what these respondents consider as their greatest threat to business technology operations, “ransomware” and “human error” tied as the top concerns. These responses indicate a neglect for the restorative side of IT practices, especially when the noted top threats demand a restorative strategy to mitigate. Put together, this could mean organizations are potentially at significant risk.

Assessing Your Current Strategy

To tighten up your IT stance, Bluelock has detailed a few questions below to ask yourself as a self-assessment of current IT practices. The answers will help to identify any gaps that might exist in your current program.

Prevention

1 Has your organization established a Risk Profile?

The goal of establishing a Risk Profile is so that stakeholders can fully understand the vulnerabilities your organization currently faces and determine if it is a desired risk tolerance. The analysis necessary to determine a Risk Profile should include board and executive interviews, operational risk assessments, application inventory, third-party risk assessments and discussions with each business unit.

2 What prevention strategies have you implemented?

Your organization should have a variety of technologies and policies to stop intrusions and disruptions: threat management (encryption, vulnerability scanning, patching); access control (user access, multi-factor authentication or MFA, password policies); and end point protection (antivirus, anti-malware, firewalls, mobile device management (MDM), user training). It’s also key to continually update these technologies. All employees should be required to participate in technology training programs, no matter their level within the organization, to learn about proper usage of internet and email, confidentiality, data storage and protection, documentation and social media. This will make enforcement an easier process.

Detection

1 Do you have a log monitoring process that includes logging, monitoring, threat identification and response?

For every IT system, you want to log all changes that occur, who made them and when. But it goes beyond that too: organizations should review the logs and correlate those records against other logs to identify threats, separating the signal from the noise. From there, IT can accurately respond to emerging incidents. This level of security and scrutiny will also assist in customer, auditor or stakeholder inquiries.

2 Do you regularly monitor and test for penetrations & vulnerabilities in your IT systems?

Tracking the real-time status of your IT systems requires vigilant attention to your network and where your data lives. This means eyes should be searching for unwarranted changes at all times. In addition, you should go beyond simply monitoring your IT systems to performing regular scanning tests to identify penetrations and vulnerabilities, as this will help to ensure all gaps are addressed.

This type of monitoring and testing also provides a feedback loop into prevention. Identification of vulnerabilities is only part of the equation: what you do with the information is the real goal. Do you ensure all vulnerabilities receive action? Does this information feed your patching process? Do you have clear responsibilities delineated between IT personnel?

Restoration

1 Does your organization have a policy for business continuity? If so, how often is this policy renewed, tested and updated?

First and foremost, it is key to have an overall process in place, beyond IT systems, to ensure continued operations after an event. This could include a robust Public Relations strategy, notification process for all employees, etc. It's paramount to consider all likely and unlikely events and have a plan in place to address

and recover from each. IT disaster recovery (DR) and security incident response plans should fall under the same umbrella and be managed by the same team, since event scenarios often overlap in impacts, and thus require similar response tactics and objectives.

2 Is there a formal process to gather and prioritize applications based on how they support business?

Perform a business impact analysis (BIA), either internally or via a third party. It's key to inventory everything and understand the intricacies of each dataset and application. This assessment will uncover what things are interconnected and dependent on one another. Create a map of these dependencies. When an event happens, what gets first attention? Why? What's next, and so forth? Document the answers to every possible question. Look beyond initial boot order to the quality assurance aspects as well, which are often forgotten during an event, but are imperative for a timely recovery.

3 Do you have a management process for incidents or breaches?

As part of your IT disaster recovery plan, maintain an IT disaster recovery playbook. This document will be the single source of information to recover IT systems and data after an event, noting all roles, responsibilities, processes and configurations. Ensure all staff members have the ability to anonymously report incidents, and your IT team has the ability to effectively track and resolve all incident reports quickly. If a third-party investigator is needed, it's good to have a process to communicate with this person or entity. Perhaps most importantly, there should also be a notification process documented to let stakeholders, leadership, customers and other constituents know what's happened and how it's being resolved.

IT disaster recovery (DR) and security incident response plans should fall under the same umbrella and be managed by the same team.

4 Does your organization routinely test its IT disaster recovery and incident response process?

Every organization should test their DR plan once every six months. It's important to perform a variety of assessments as well, from sandbox testing, tabletop testing, to a full or partial failover test. Since different scenarios could mean different recovery processes, it's also necessary to test for different roadblocks, like if key IT members are absent. Test beyond the data too, looking for networking and connectivity issues, as this is the most encountered problem in an actual event. After each test, the IT team should review the results and coordinate updates to the Business Continuity, Incident Response and DR plans.

5 Which of these strategies have you implemented: archiving, backups, snapshots, replication?

You should have at least three copies of your data, each on different media and at least one of these iterations off-site. But the answer to the above question should be all of them. Why? Backups are for data protection and restores, not necessarily for large-scale recovery. Each of these solutions represent a different purpose and speed of recoverability. Having all of them allows for flexibility and full coverage against a spectrum of disasters and cyber threats. Organizations should have different backup strategies for archival data versus production data. For example, if data is needed to run day-to-day business, then copies (with multiple, time-stamped iterations) need to be readily accessible in case of need.

Strengthening Your IT Stance

Good preparedness for disasters and cybersecurity incidents requires mitigation against every threat. If you find the preventative and detection questions difficult to answer, you might want to speak with your IT team and any third parties to ensure all precautions are in place to identify and stop events. If you're using the cloud in any way, even a SaaS application, know that this will entail shared responsibilities – do you know where the delineation lies? A cloud provider should be able to do a number of preventative and detection measures on their end, and be sure to request documentation of these actions for your records.

If you can't answer these restoration-focused questions easily, you might want to consider Disaster Recovery-as-a-Service (DRaaS), a solution that keeps data safe in a third-party environment to enable the transfer of operations during a disaster event or unexpected disruption. Organizations are able to quickly spin up data and systems in a secure, production-grade cloud from which they can run operations, mitigating the risk of downtime and reputation degradation.

What can DRaaS do?

- Empower fast recovery during a disaster event or outage
- Gain secondary datasets for security breach response
- Secure data storage in a dedicated datacenter
- Give documented proof of testing and recoverability to constituents
- Extend your IT team with a team of experts
- Enable failover AND failback to recover from an event

Bluelock has been named a leader of DRaaS, both by analyst firms and clients. See why we excel at recovery solutions, and read our client reviews on G2 Crowd.

*To speak with an expert about your DR strategy, drop us a line at Bluelock.com to schedule a conversation or call **888-402-2583**. A quick 30-minute phone call will help us jointly discover how DRaaS might improve your DR strategy.*

Read Bluelock's Practical Guide to DRaaS

The Practical Guide to Disaster Recovery-as-a-Service is a beginner's resource for understanding the end-to-end aspects of tackling IT resiliency.

- Learn how to gain company-wide buy-in
- Understand the 3 types of DRaaS service models
- Tier your applications for expedited attention during crisis
- Test your DR solutions for success
- Get tips for a successful DRaaS implementation

Access Now