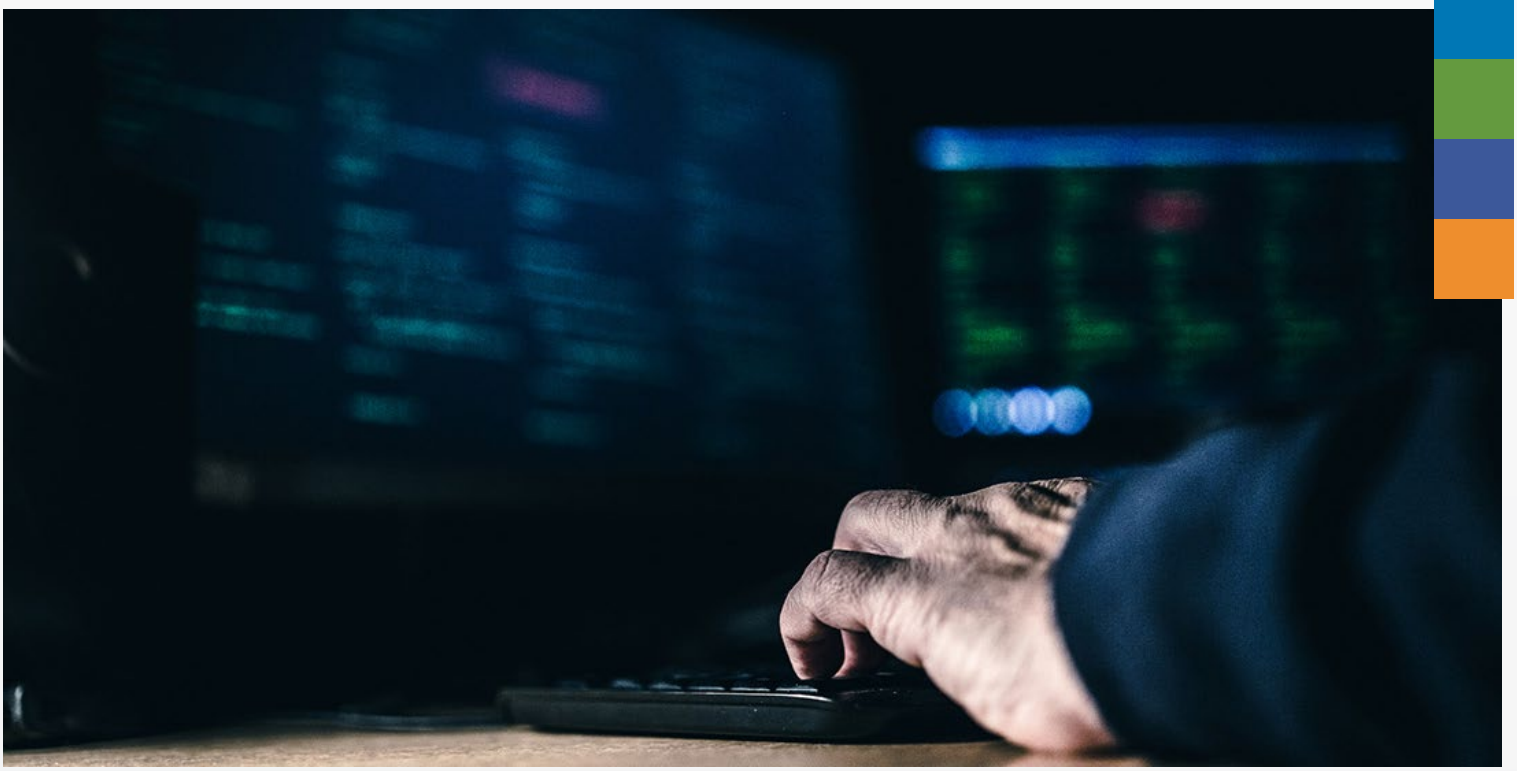
PathForward IT
Founding partner of BLUE ALLIANCE IT

Resources /
Blog

Back Up Your Data to Get It Back From A Cyber Attack

4 minutes read



Today's accelerated technology trends are powering unprecedented business transformation. But they're also introducing an overwhelming amount of security risk. Hackers use a wide range of tools and methods to gain access to your data—from social engineering and phishing scams to ransomware attacks and exploiting systems vulnerabilities. With virtually all personal and business data stored on internet-connected platforms, targeting businesses has become a gold mine for bad actors. To ensure the best chance of business continuity following any compromising cyber event, *strategically* backing up your data is one of the most foundational best practices you should include in your layered security checklist.

siness-Critical Backup and Recovery, Without A Plan

Cybersecurity professionals agree pretty much universally that, it's not a matter of whether businesses will encounter an attack, but *when*. Trying to execute every-day business functions, without access to data, is like trying to drive a car without the tires—basically, inoperable. The very purpose of an holistic security strategy is to minimize as many gateways available to threat vectors as possible; local (on-prem locations), geographical distribution (networked systems) and cloud backups (primary or redundant data storage) are fundamental first steps in a layered approach to protecting your data.

Unfortunately, employing a data backup strategy isn't as universally agreed upon. If that sounds contradictory, well, it is. In fact, even many IT professionals generally view backups as an insurance against the *potential* for an attack verses a priority to *combat* attacks. But consider this common scenario: a company has recognized the importance of backing up data and engages IT to deploy it. A random device is selected and turned on in a single location, but never tested, runs on subpar hardware, and has no particular defined parameters. This approach has a very different outcome during recovery from a cyber attack than a strategic data backup solution.

Business Continuity Predicated on Data Recovery

If you're employing a set-it-and-forget-it backup strategy, you're in for a rude awakening when an incident occurs. Waiting until you need your backups is, arguably, the worst time to wonder how many copies of your data are available and where and how they're stored. During an incident, time is critical; downtime adds up quickly and can be extremely costly to your customers, your reputation, and your bottom line. Some businesses simply can't recover; they go out of business. For a significant outage, you need to be able to act fast and be responsive. If you, or your solution provider don't know what you don't have, you're looking at a substantial amount of downtime, and mounting associated recovery costs, as you work it out.

Making Cybersecurity A Priority with Data Backup

Companies are best positioned to assure business continuity if each of these steps have preceded an incident:

- **Security-minded culture:** user behaviors and policies awareness; ongoing compliance reinforcement
- **Preventative measures:** annual third-party security assessment to document vulnerabilities in the security controls, along with correction recommendations; firewalls and backup strategy functioning as intended; allow listings and access controls implemented; timely patching; audits, testing, monitoring, and spot checks; and fire drills to ensure everything is documented and security settings haven't changed
- **On-call service in place:** 24/7/365 fully-staffed, live helpdesk of experienced, certified engineers with a 15-minute disaster response time

Off-loading some of the routine tasks associated with cyber hygiene like software updates, patching, testing, and backups to an MSP like *Path Forward IT* is an investment in your overall security plan. This simple step enables a service provider, with end-to-end data protection solutions, to get to know your systems environment intimately, enabling expert counsel for when you need to make operational changes that impact IT, are thinking about a purchase decision, or encounter an attack or natural disaster.

Backup Options Matter

Of course, you never want to get to recovery mode, but when you do, the quality of your backups will be very important. The best mitigation for destructive cyber-attacks is having rock-solid backups. However, with the advent of *affiliate ransomware*, attackers will now go after any accessible backups too. This makes a secure cloud-based backup solution a good choice—one that uses authentication that requires a unique set of complex credentials for access (does not overlap with workstation, server, or domain credentials) and does not require physical servers in the event of a disaster. What makes *Cohesity* enterprise-class backup solutions the preferred choice of so many enterprises worldwide are the expanse of options available to prepare your organization for a variety of data compromises. *Cohesity* provides a secondary repository with immutability, for offsite storage, ransomware early detection, and other advanced security features, along with a team behind it, monitoring and testing everything daily to ensure its efficacy.

The benefits of backup options become crystallized during a recovery operation. Customized data protection and recovery solutions provider, *Path Forward IT*, points to less production impact and downtime in general, rapid speed to restore, massive data storage of up to 35 PiB (pebibytes), granularity, and the flexibility to scale and customize the solution to fit customer needs.

Backup As Last Line of Defense

A layered security strategy improves your chances of stopping threats from penetrating your environment. But as new technologies develop and threat actors mature in finding ways to exploit them, strategically backing up your data can mean the difference between business devastation and a quickly-contained service interruption.

> *"If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it."—Tim Cook, CEO, Apple Inc.*

To learn more, request a consultation with *Path Forward IT*.

—

Resources

Top 25 Cyber Security Threats

Ransomware Attacks are not a Matter of If, but When

RPO / RTO

Six Stages of Penetration Testing

Related Insights

BLOG

What Most People Don’t Know About Cyber Insurance

Read >

BLOG

Reduce Your Ransomware Risk with Allow-Listing and Other Application Execution Control Solutions

Read >

BLOG

How a Backup and Recovery Audit Can Safeguard Your Business

Read >

Solutions

Managed Services

Data Protection

Connected Business

Cloud

SaaS

Audio/Video

Advisory Services

Compliance

Customized Project Engagement

Business Application Support

Industries

Healthcare

Manufacturing

Finance

Education

About

Our Company

Careers

Request a Consultation

Contact

Resources