eBook

Axcient

Cyber Insurance Guide for MSPs

Using Automation for Cyber-Insurability

Is Your MSP "Cyber-Insurable?"

MSPs are under attack and must have the support of a policy that matches your risk.

Cyber Insurance is relatively new, but with increasing cyber threats to small to medium-sized businesses (SMBs) – especially Managed Service Providers (MSPs) – it's gotten harder to get coverage. MSPs are under attack and must have the support of a policy that matches your risk.

To become cyber-insurable, MSPs must meet the requirements of their desired policy. Policy applications can reach over 20 pages and demand substantiation of backup and disaster recovery (BDR) capabilities. Depending on your BDR solution, the thoroughness of your business continuity plan, and your ability to recover after an incident, qualifying for coverage and getting claims paid can be simple or complicated.

Contents

In this eBook, we're giving MSPs answers so you can take the easy road to achieving cyber-insurability, gaining coverage, and securing compensation. Keep reading to…

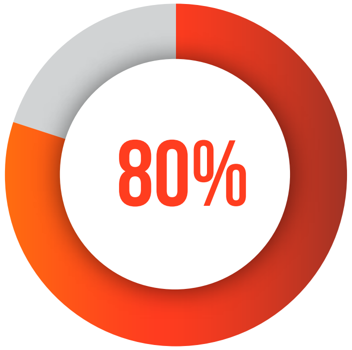
→ Weigh the costs, benefits, opportunities, and risks surrounding cyber-insurability to **optimize security-first disaster recovery planning, compliance, and sales and marketing.**

→ Learn what's typically demanded of MSPs during the application phase and **prepare for new demands challenging the channel.**

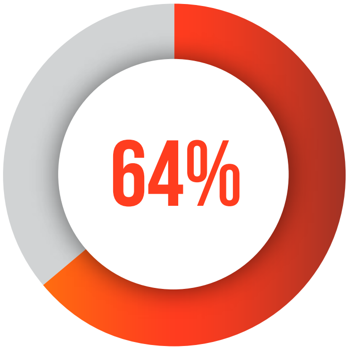
→ See how comprehensive business continuity and disaster recovery (BCDR) **enable cyber insurability and time and labor savings with automation.**

→ Take the "Are You Cyber-Insurable? Quiz at the end of the eBook to **assess your MSP's ability to qualify for cyber Insurance.**

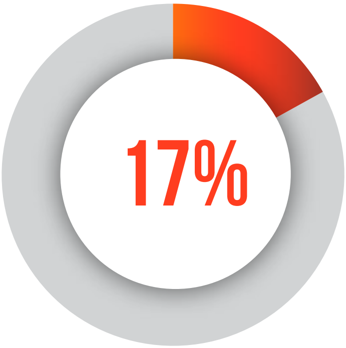
Too Many MSPs Are Risking Their Businesses – Are You One?



80% year-over-year increase in ransomware.



But… 64% of small business owners aren't familiar with cyber Insurance at all.



And only… 17% of SMBs have enough cyber Insurance to cover the average cost of a breach.

$157,000 is the average incident cost for SMBs.

81% of cyber claims involve recovery expense losses.

1. Ransomware
2. Hackers
3. Email Compromise
4. Human Error
5. Phishing

LOSSES IN THESE 5 CATEGORIES ACCOUNT FOR 70% OF CLAIMS AND 80% OF COSTS.

Resources:

Zscaler ThreatLabz 2022 Ransomware Report
AdvisorSmith Report
NetDilligence 2022 Cyber Claims Study

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

What is Cyber Insurance?

Cyber Insurance or cyber liability insurance helps businesses cover financial losses due to cyberattacks or data breaches involving sensitive information.

Policies offer different types of protection based on what scenarios the business wants to receive compensation for after an event occurs. When evaluating your needs, consider today's threat vectors, your ability to tolerate downtime, the impact of forgoing coverage, and your budget for premiums and recovery expenses. At the bare minimum, MSPs need "must-have coverage." However, getting a policy that protects you from the costs you're most likely to incur is best.

Must-Have Coverage

- Data breaches.
- Cyberattacks on your data.
- Cyberattacks on your client's data.
- Cyberattacks on any data stored with vendors and other third parties.
- Cyberattacks that occur anywhere in the world – not just the U.S.

Recommended Coverage

- Cyber extortion, including ransomware and social engineering.
- Regulatory fines or penalties.
- Media liability and reputational losses.
- Business interruptions and downtime.
- Breach response and management expenses.

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

Why Do MSPs Need Cyber Insurance?

Cyber Insurance is a safety net like health insurance, car insurance, homeowners' Insurance, etc. However, unlike those other types of Insurance, MSPs are not required to have cyber Insurance to do business. Some see this as an opportunity to cut costs and stick their head in the sand.

We aren't trying to scare you – if you are reading this eBook, you may realize that you need to both secure your client's data and be realistic about the level of risk you are taking on.

→ **High risk.**

→ **No recovery costs are covered.**

→ **No external assistance.**

→ **No compliance penalty compensation.**

Proactive MSPs Need Cyber Insurance

Taking a security-first approach to business continuity and disaster recovery means you're proactive, realistic, and prepared for whatever is possible. (Check back to page 3 for a reminder of what's possible – and probable!)

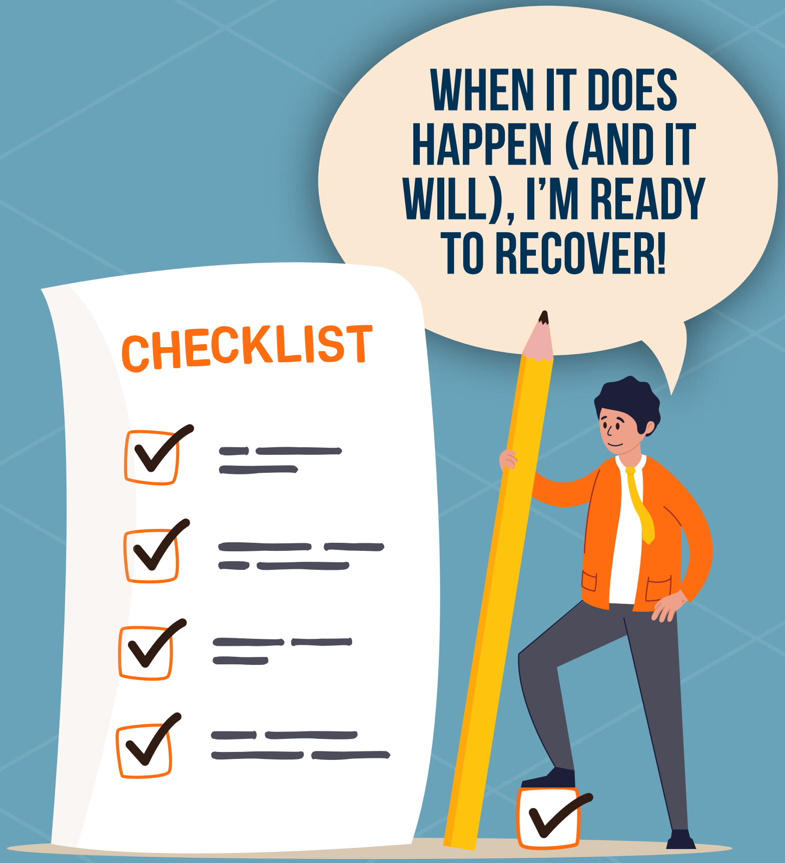
→ **Low risk.**

→ **Recovery cost coverage.**

→ **Third-party support.**

→ **Compliance fine assistance.**

Consider the following questions as you assess your risk, evaluate carriers and policies, and weigh premiums against risk tolerance and budget…



Can You Cover the Cost of a Breach?

There’s no limit to what a cyberattack or data breach could cost your MSP. That’s the thing about cybersecurity – you don’t know what’s coming – and that’s what cyber Insurance covers.

→ **Expenses to restore normal operations** and repair reputable damage – additional labor and disaster recovery tools.

→ **Replacing damaged property –** computers, laptops, mobile devices, and backup hardware.

→ **Notifying customers** of the breach and communicating recovery processes.

→ **Lost business income** due to downtime during and after the incident.

→ **Legal fees** for compliance breach notifications and potential litigation if the MSP is sued.

→ **Third-party damages** from clients, vendors, and other stakeholders who suffered a loss due to the incident.

→ **Fines** imposed by regulatory bodies like GDPR and HIPAA.

→ **Public relations efforts** to manage reputational damage to the MSP.

→ **Forensic investigation** to assess the incident, identify vulnerabilities, and mitigate future risks.

All or none of these costs could be covered depending on your cyber Insurance.

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

Do You Have the Legalese to Communicate a Breach?

After a cyberattack or data breach, MSPs can be quick to want to (or have to) communicate with clients, internal and external stakeholders, the public, and compliance agencies. While the intention is to ease fears and reassure, speaking without legal counsel can put your MSP at legal risk.

Communicate carefully! Using the words “breach,” “incident,” “attack,” “intrusion,” or “hack” all carry different implications, and using the wrong term publicly could open your MSP to undue liability or litigation.

When you have cyber Insurance, there are 2 reasons that you MUST first call your carrier after an incident – before doing anything else:

Acting without the direct advisement of your cyber insurance provider could result in denied claims or legal ramifications.

You will be assigned a Breach Attorney or Breach Coach who will guide you through disaster recovery communications from a legal standpoint. This is typically included with most plans.

Get compensated and avoid additional costs and stress after a cyber incident.

Can You Meet Compliance Standards?

Cybersecurity Maturity Model Certification 2.0 (CMMC) is introducing new requirements for MSPs handling sensitive data on behalf of the Department of Defense (DoD), including:

→ **Demonstrate proof of regular backup testing.**

→ **Meet Governance, Risk, and Compliance (GRC) framework needs.**

→ **Utilize automation over manual intervention.**

Unsurprisingly, the federal government is establishing similar guidelines.

Breach notification laws in all 50 states require businesses to notify consumers or citizens within a specific time period and according to procedure if their personal information is breached.

Breach notification rules also exist for compliance agencies like HIPAA, FINRA, GDPR, and others.

Failure to comply with these varying standards can result in fines, penalties, and potential litigation.

What the Overlap of Insurability and Compliance Means for MSPs…

!

→ **The legal support of an insurer helps reduce your chances of incurring further damage through compliance penalties.**

→ **Having cyber insurance could mean that you're already meeting the standards of CMMC (depending on what your carrier requires). Kill two birds with one stone – cyber-insurability and compliance!**

→ **Fines may be covered by your policy.**

Are You Missing Out on Sales?

Cyber-insured MSPs have a leg up on their uninsured competition. To meet the qualifications for cyber Insurance, MSPs must show off the best of their data protection skills. In doing so, you're creating the bones of a cybersecurity sales and marketing campaign.

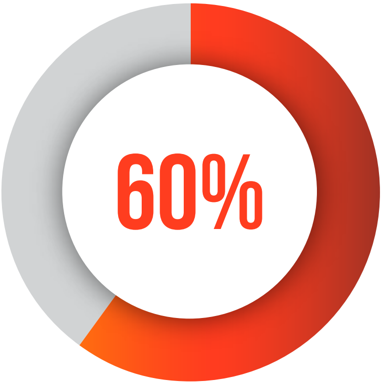
→ **Highlight the benefits of choosing an MSP with cyber Insurance** by educating clients and prospects about cyber-insurability for MSPs.

→ **Leverage the security requirements you have met** and will continue to meet for cyber Insurance as another layer of protection for clients.

→ **Expand your BCDR services** by sharing proof of regular backup testing with clients.

→ **Regularly reinforce your security-first approach** to BCDR when new reports are generated for ongoing security checks and your policy is renewed.

Give prospects and clients more to say YES to.



60% of businesses report being hesitant to enter into a new agreement with any organization lacking cyber insurance.

Resources:

BlackBerry and Corvus Insurance, How Cybersecurity Insurance Provides Protection, 2022

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

How Do MSPs Get Covered?

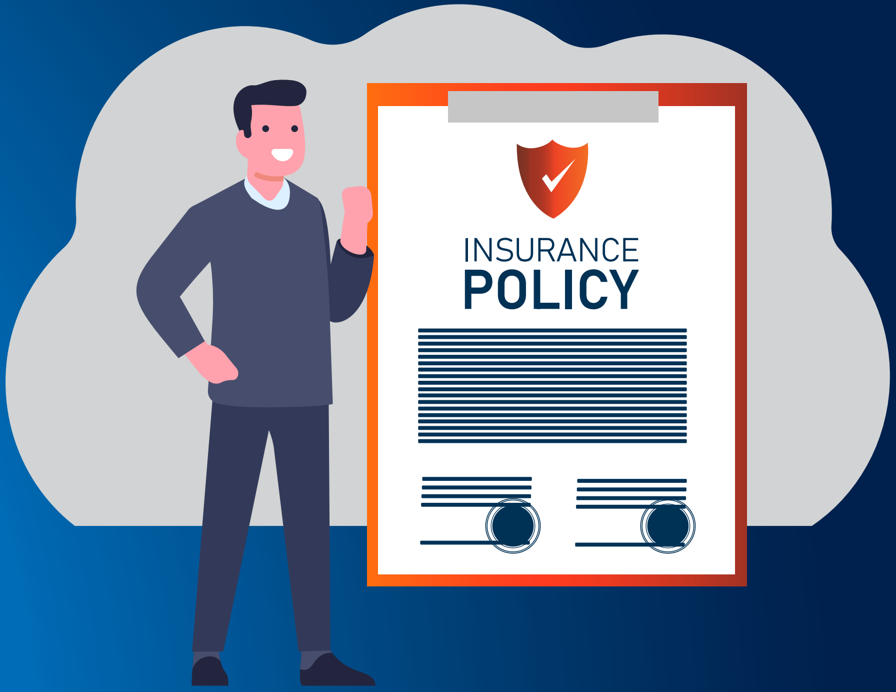
Again, policies vary, but some general minimum requirements for MSPs include…

→ **Multi-factor authentication (MFA) on all admin access and privileged accounts >** To do that, MSPs need to visualize users across security products.

→ **Demonstrate proof of regular backup testing >** To do that, MSPs need to test backups daily with evidence of results.

→ **Demonstrate proof of cybersecurity best practices >** To do that, MSPs need to utilize automation, high visibility reporting, stack consolidation, and efficient BCDR management.

Your ability to meet these requirements quickly, completely, and cost-effectively largely depends on the features, capabilities, and level of maturity delivered by your backup and disaster recovery tools.



Legacy BDR vs. Modern BCDR

- Additional time and resources for MFA.
- Time-consuming daily manual backup checks with manual reporting.
- Increased risk of cyber incidents due to human error = Higher premiums or policy disqualification.
- Higher recurring costs for additional labor requirements and operations.

- Built-in MFA.
- Built-in, automatic daily backup checks with automated reporting.
- Lower risk of cyber incidents with automation = Lower premiums and cyber-insurability.
- Reduced recurring costs with time and labor-saving technology and a unified platform.

Business Continuity and Disaster Recovery for the Win!

Let’s see how it’s done…

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

AutoVerify

Automatic Backup Integrity Testing

Built-in, always-on, automatic backup monitoring, verification, and reporting means…

→ **No wasting time, labor, and money** on repetitive manual backup checks.

→ **No suffering "backup burn"** even when you see the green check mark.

→ **No worrying that backups won't boot** during an incident.

How AutoVerify Supports Cyber-Insurability:

→ **Demonstrate proof of automation and daily backup testing** with custom-generated Backup History Reports going back up to two years.

→ **Automatic self-healing response** detects backup failures and automatically re-backups up the compromised portion of the data in the next backup.

→ **Custom alerting and escalation rules** route notifications to the assigned parties for follow-up and remediation.

Organizations that fully deploy cybersecurity automation experience

108-DAY SHORTER

breach lifecycles and nearly

$1.8 MILLION

lower data breach costs compared to organizations not deploying these technologies.

Resources:

IBM, Cost of a Data Breach Report 2023

Virtual Office from Axcient

Self-Managed Cloud Disaster Recovery

Built-in, always-on cloud failover that instantly recovers production servers and workstations by starting virtual machines in the Axcient Cloud of one or more protected devices to replace all impacted systems temporarily.

→ **Create automatic deployments for client-specific virtualized devices** using pre-configured runbooks for rapid virtualization in a disaster or for testing.

→ **Get Virtual Office for free for 30 days every year** to deliver uninterrupted business continuity despite equipment lag times and physical office damage.

→ **Contain usage and maximize free days** with custom controls that automatically shut down test instances based on your settings.

How Virtual Office Supports Cyber-Insurability:

→ **Demonstrate proof of disaster recovery testing** with regular, full-office disaster tests and frequency documentation.

→ **Automatic runbooks** enable testing efficiency to ensure backups are recoverable and you're meeting your policy's testing automation requirements.

→ **Secure access and data encryption** using VPN, Site-to-Site OpenVPN, and port forwarding to our offsite SOC II Type II certified data centers.

Anti-Ransomware and Data Loss Technology

Built-in, always-on data loss protection that automatically separates data deletion requests from the mechanics of data deletion to prevent accidental and malicious permanent data loss.

→ **Limit who can create and fulfill data deletion requests** – and stop any one individual from completing both tasks – with human factor controls.

→ **Secure your data deletion process** by requiring human two-factor authorization via audible approval from an authorized representative before data deletion requests can be fulfilled.

→ **Sleep soundly,** knowing you can always restore data from safe and protected snapshots – even after a ransomware attack.

How AirGap Supports Cyber-Insurability:

→ **Automatic ransomware protection** demonstrates your understanding of threat vectors and commitment to cybersecurity best practices, thus lowering risks for insurance carriers.

→ **Time gaps** between when data deletion requests are created, verified, and executed all vary in length to avoid recognizable patterns that bad actors can replicate and exploit.

→ **Honeypots** prevent further damage by tricking hackers into thinking they've successfully accomplished their attack, but it's just an illusion to send them on their way.

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

x360 Recover

Modern Business Continuity and Disaster Recovery (BCDR)

The most comprehensive, flexible, and cost-effective BCDR solution built specifically for MSPs to consolidate stacks efficiently, streamline management, reduce downtime, and significantly cut costs.

→ **Cover most use cases with just one solution –** including endpoint backup, hardware-free BDR, full-service BDR, and public or private cloud backup.

→ **Replace legacy chains with proprietary Chain-Free backups** to eliminate reseeding, consolidation, and storage overages in favor of time and labor savings, long-term retention, and worry-free storage.

→ **Get AutoVerify, Virtual Office, and AirGap** for uninterrupted business continuity, rapid recovery, and ransomware roll-back – all built-in and always on!

How x360Recover Supports Cyber-Insurability:

→ **Automatic** backup integrity testing, runbooks for immediate cloud failover, and permanent data loss protection lower your risk and increase your chances of gaining affordable coverage.

→ **Documented** proof of BDR testing through automatically generated reports simplifies long application processes and ongoing security checks.

→ **Modern** BCDR includes critical capabilities and innovations that evolved from legacy BDR to meet the threat vectors of today's cybersecurity landscape.

Checklist: Are You Cyber-Insurable?

Now that you know what cyber-insurability is, why it's so crucial to your MSP, and how to meet cyber-insurance standards – are you cyber-insurable? Answer the questions below and total your score to assess your cyber-insurability.

1. **Can you demonstrate proof of regular backup testing?**
   - □ Yes, with automatic backup testing and custom-generated backup reporting. (+3)
   - □ Yes, with manual backup testing and hand-generated results. (+2)
   - □ No. (+1)

2. **Can you demonstrate proof of regular disaster recovery testing?**
   - □ Yes, with automatic, pre-configured runbooks and frequency documentation. (+3)
   - □ Yes, with manually implemented disaster recovery tests and hand-generated reporting. (+2)
   - □ No (+1)

3. **Do you have visibility into backup management through reporting and dashboards?**
   - □ Yes (+3)
   - □ Some (+2)
   - □ No (+1)

4. **How many backup and disaster recovery solutions and vendors are in your stack?**
   - □ 1-2 (+3)
   - □ 3-4 (+2)
   - □ More than 4 (+1)

5. **What kind of backup technology are you using?**
   - □ Chain-Free (+2)
   - □ Chain-based (+1)

6. **How often is automation used in your backup and disaster recovery processes?**
   - □ More than 50% (+3)
   - □ About 25% (+2)
   - □ Less than 15% (+1)

7. **Can your backup solution automate self-healing after a backup failure?**
   - □ Yes (+2)
   - □ No (+1)

8. **Do you use custom alerting and escalation rules for risk mitigation?**
   - □ Yes (2+)
   - □ No (+1)

9. Do you have ransomware roll-back or permanent data deletion protection enabled?

   □ Yes (+2)

   □ No (+1)

10. Are your or vendor's data centers SOC II Type II certified?

   □ Yes (2+)

   □ No (+1)

11. Do you have multi-factor authentication (MFA) on all administrative access and privileged accounts?

   □ Yes (+2)

   □ No (+1)

20-27 points = Cyber-Insurable and Proud!

If you don't already have cyber Insurance, your MSP is ready to start evaluating policies and applying for protection. You've got the cybersecurity, risk mitigation, and business continuity strategies carriers want to see from MSPs. With your level of automation and consolidation, proving your capacity to meet standards will be simple and efficient for ongoing protection, support, and guidance in the event of a cyber incident.

CYBER INSURED

15-20 points = Almost There…

Consider what's keeping you from becoming cyber-insurable and identify the lowest-hanging fruit. Automation is powering many features that make cyber-insurability possible, so if that's not available in your current BDR solution, you may be inhibited by a legacy product. If you have multiple solutions and vendors in your stack, visibility into backup and disaster recovery systems may be limited. As you move toward cyber-insurability, evaluate your solutions as well as you're using them. Don't be afraid to explore your options in the market – making a switch could get you more than just cyber Insurance.

Below 15 points = Time to Make a Switch.

Unfortunately, your backup and disaster recovery solution might be unequipped to deliver the modern requirements of high-risk businesses like MSPs. BDR solutions that fail to provide the business enablement necessary for cyber-insurability pose a significant threat to your business. Backups are in danger of failure, disaster recovery is slowed, operational costs are high, and if customers haven't started to notice, they soon will. It's time to upgrade from legacy BDR to comprehensive BCDR.

CYBER-INSURABLE?
CONTENTS
WHERE WE ARE
CYBER INSURANCE 101
WHY INSURE?
BE PROACTIVE
COST
LEGAL
BE COMPLIANT
INSURABLE COMPLIANCE
SALES
GET COVERED
MODERN BCDR SUPPORT
AUTOMATE BACKUPS
SELF-MANAGE DR
STOP DATA LOSS
EVOLVE TO BCDR
ARE YOU CYBER-INSURABLE?
RESULTS
PROTECT EVERYTHING

Become Cyber-Insurable with Axcient

Axcient x360Recover is a single, reliable, easy-to-use BCDR platform designed to satisfy nearly all MSP use cases with the cybersecurity and automation demanded by cyber insurance carriers. As a 100% MSP-only solutions provider, Axcient is dedicated to helping MSPs keep businesses running – including their own. Here's how we do it…

Flexible Deployment Options: Solve multiple use cases with just one solution and one vendor – including endpoint backup, hardware-free BDR, full-service BDR, and public or private cloud – plus robust **BYOD/C capabilities.**

AutoVerify: Automate nightly backup integrity checks and reporting without manual intervention.

Virtual Office: Automatically virtualize backups with customizable runbooks for near-instant recovery.

AirGap: Automatically separate data deletion requests from the mechanics of data deletion to always recover – even after ransomware.

Local Cache: Accelerate cloud recovery and let missing data blocks self-heal so you can sleep soundly.

Proprietary Chain-Free Backups: Solve for data bloat and eliminate the pains of legacy, chain-based backups – no reseeding or consolidation.

Pooled Storage for a Flat Fee: Simple pricing per device and server.

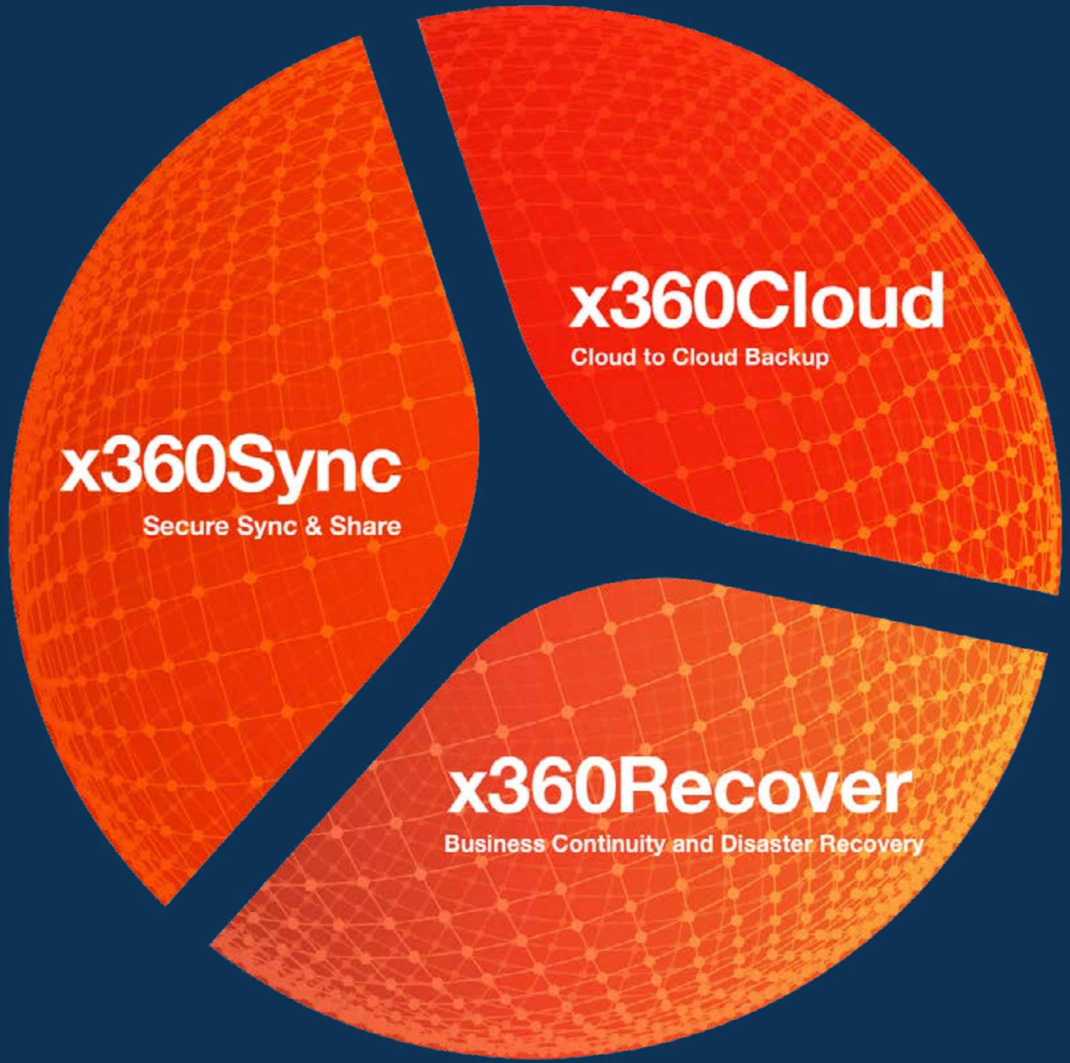
Customization and Choice: Customers can BYOD, purchase or lease appliances from Axcient – and BYOC or data center, or replicate to the secure Axcient Cloud.

See how Axcient **x360Recover** supports cyber-insurability with comprehensive BCDR.

Schedule a 1:1 Demo

or

Start Your FREE 14-Day Trial Now!



x360Cloud

Cloud to Cloud Backup

x360Sync

Secure Sync & Share

x360Recover

Business Continuity and Disaster Recovery

About Axcient

Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 3,000 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com

Axcient