eBook

Axcient

5 Critical Pieces of a Good Cybersecurity Playbook

Axcient

Introduction

Cybersecurity today requires much more than just backup and disaster recovery. For MSPs to ensure business continuity for their SMB clients, they need a comprehensive plan covering both the immediate and long-term effects of a cyber incident. A properly designed cybersecurity playbook assumes that data loss will occur and provides reassurance that the business will survive regardless of how the data is lost. This eBook answers the most critical questions surrounding recovery, including:

- **How do I approach immediate and long-term planning for incident response and recovery?**
- **What is the difference between an incident response (IR) plan and a business continuity (BC) plan?**
- **What are the considerations for Cyber Liability Insurance?**
- **What are the five critical pieces of a good cybersecurity playbook?**
- **How do I get started?**

Table of Contents

IR Plan + BC Plan = Cybersecurity Playbook

A cybersecurity playbook is an all-encompassing, organization-wide manual that dictates precisely what actions to take when data loss occurs. It combines an incident response plan (IR plan) with a business continuity plan (BCP) to guide you through a cyber incident from initial discovery to preventing a reoccurrence. Sometimes these plans can be incorrectly referred to interchangeably, but the significance of differences is key to creating an ironclad cybersecurity playbook.

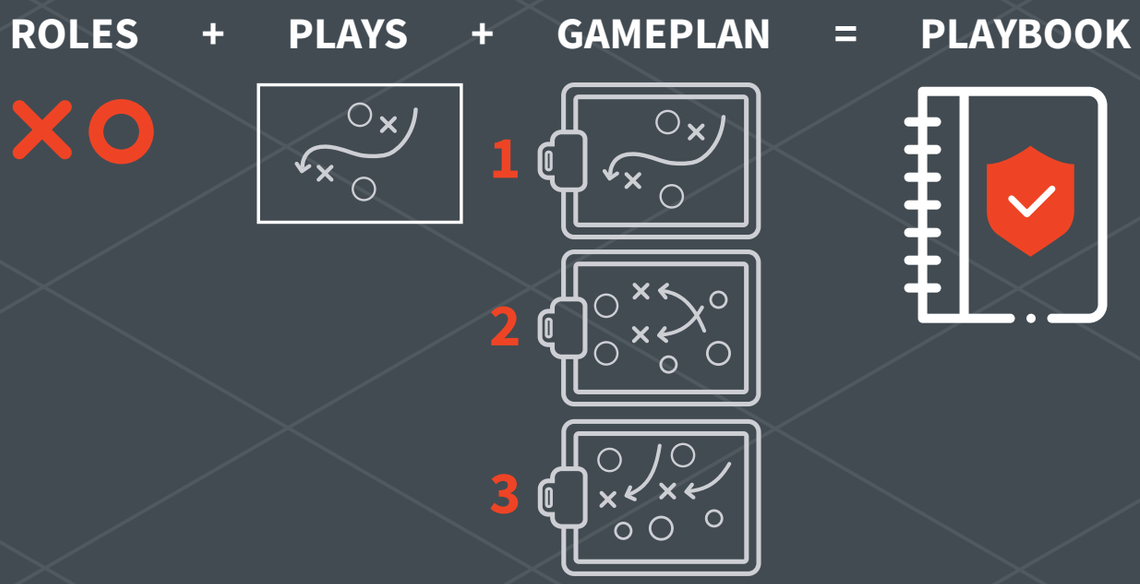


Table of Contents

Immediate and Long-Term Planning

Incidence Response (IR) Planning

Imagine that a cyber incident has just occurred. Whether it's a natural disaster, a ransomware attack, accidental data deletion, or a critical device is lost, stolen, or destroyed; your IR plan answers the question, 'what now?' IR policies tell you exactly what to do in the event of a breach. An incident response plan documents the answers to 'what now?' with a detailed, practiced, accurate, and comprehensive roadmap from breach discovery to complete restore.

Your IR plan should then extend through investigation and policy updates. Once established, mock disasters and table reads of your IR plans should lead to regular updates to accommodate internal changes, current security threats, system upgrades, and changing state, federal, and industry regulations.

IR Response Team

One facet of an IR plan that can be overlooked is your incident response team members. These are the first people to be contacted who will then complete the tasks outlined in your cybersecurity playbook. Once the incident has been discovered, the team is responsible for the following:

- → Assessing the damage and determining whether tools need to be shut down – essentially, 'stop the bleeding.'
- → Tracking the incident
- → Contacting the cybersecurity insurance provider and/or lawyer(s)
- → Coordinating with insurance-approved IR provider
- → Outreach to affected customers
- → Compliance with breach notification regulations (i.e., HIPAA, GDPR, state laws, etc.)

Table of Contents

Business Continuity (BC) Planning

A BC plan takes over once the initial IR plan is already in motion. It defines how a business will continue running while the IR plan is moving, despite a crisis situation. For example, your **cyber liability insurance** provider will most likely conduct forensics following a breach to determine the payout of your claim. Your BC plan provides a resolution for doing business despite being locked out of your systems.

Every BC plan should include the following:

- An in-depth audit of the various risks, threats, and problems most likely to impact business operations
- Mission-critical business functions and processes that, if interrupted, will cause operations to stop
- Internal personnel who have the authority to declare a disaster and communicate with external stakeholders
- Emergency communication plan for alerting employees, vendors, and stakeholders if critical systems are unavailable and business facilities are inaccessible

Consider Cyber Liability Insurance Carefully

Unfortunately, despite frequent warnings, regular breaches, and the fatal consequences of cyber incidents, many MSPs continue to forego insurance and allow clients to remain unprotected. Insurance companies have noticed, premiums are rising, policies are more demanding, and applications are intensifying.

Cyber liability insurance financially protects businesses after a cyberattack or incident where company and/or client data is lost. Depending on your policy, cyber liability insurance can protect against claims for the following:

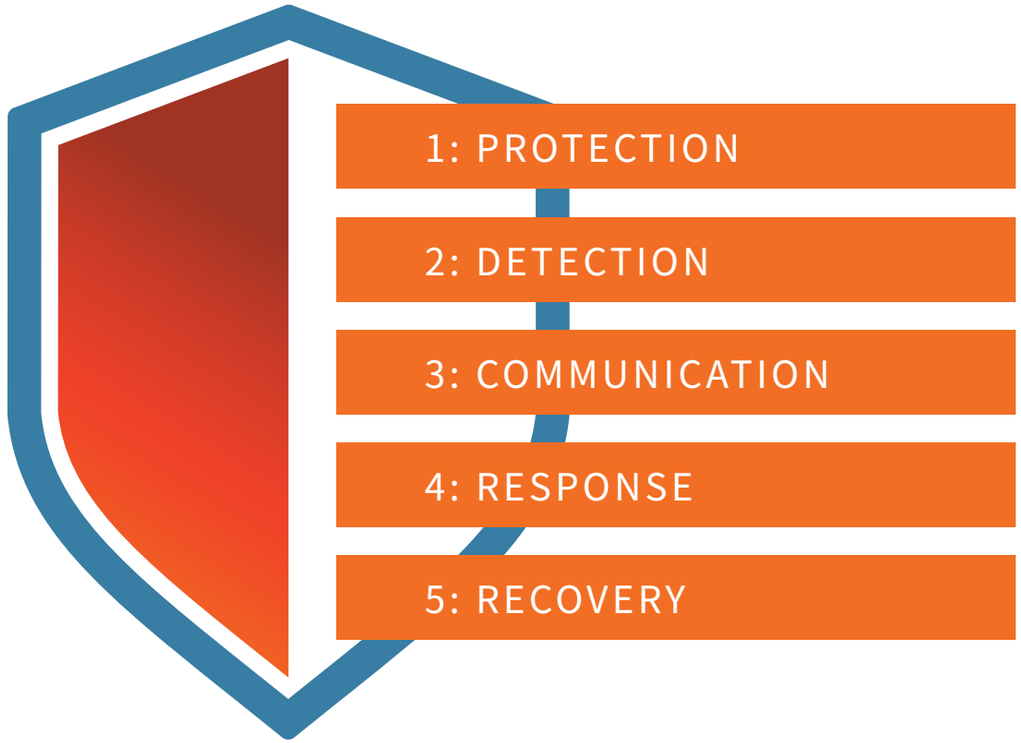
- → Regulatory fines
- → Media liability and reputation loss
- → Cyber extortion and ransomware
- → Social engineering
- → Business interruption
- → Breach response and management expenses

A big portion of a cyber liability insurance application is assessing the vendors and solutions you use, your plans for responding to an incident, and ensuring your clients have comprehensive cybersecurity protections in place.

Table of Contents

Five Steps to Preventing, Addressing, and Recovering

Put your IR plan and your BC plan together, and you've got the basis for a good cybersecurity playbook. However, good isn't good enough in today's cyber climate – it has to be downright outstanding. The five critical pieces of a cybersecurity playbook include…



#1 Protection

When it comes to a cyberattack, the adage says that it isn't a question of if but when you and your clients will be hit – but that doesn't mean you want to make it easy. You need a **layered security-first approach** to protecting business-critical data, which is the beginning and end of your cybersecurity playbook. Before and after a cyber incident takes place, you need to reassess your level of protection.

- → **What layers of security are keeping attackers out?**
- → **What threats are currently being exploited, and what protections are in place to address them?**
- → **What is your intrusion detection mechanism? What are you tracking on your network?**

These questions should be regularly discussed as part of your cybersecurity playbook practice drills, tabletop exercises, and updates.

At least quarterly, your incident response team and associated stakeholders must come together to ensure the playbook is still actionable based on the current cybersecurity landscape and business environment. Allowing a playbook to go stale could be the difference between surviving an attack or losing your livelihood.

#2 Detection

Intrusion detection, **dwell time**, and scope of compromise define the detection piece of your cybersecurity playbook. These are the tools you rely on to kick off the first actions of your cybersecurity playbook: your IR plan. They are also essential for tracking, reporting, and understanding a breach to meet compliance and regulation standards and prevent a future attack.

- **Intrusion detection:** Knowing when there's been an attack or breach. How will you be notified of data loss or suspicious activity?
- **Dwell time:** The amount of time the bad actor has been on your network or systems. With today's complex attacks, it could be months that hackers are sitting silently, penetrating systems, observing routines, and planning their attacks. When did the breach occur versus when you found out?
- **Scope of compromise:** The number of things affected or touched, the type of data impacted, and what data has been extracted. What did the bad actor do once they gained access?

#3 Communication

Streamlined communication and a clear understanding of each person's responsibilities will help you recover quickly and smoothly during a crisis. Communicating with your incident response team is critical to your immediate response. Depending on the type and severity of the cyber incident, you may not have **access to communication systems**, including phone and email. Be sure your team is ready to receive and react to emergencies through various channels.

Outside of your emergency team is the people who are authorized to coordinate and speak to external stakeholders, including clients, vendors, government and regulatory agencies, lawyers, financial personnel, and public relations. For businesses operating under compliance standards and regulations, it's vital to understand and follow breach notification policies to avoid fines and penalties. These statutes should always be revisited during quarterly updates and discussions.

#4 Response

Your cybersecurity playbook must be followed no matter the size of the incident. What may seem like a regular, contained, or minor cyber incident – for instance, clicking a **phishing** link in an email or losing a device – still needs to follow the protocol of the playbook. For efficiency, a cybersecurity playbook should have **criticality classifications** and clear directions to help define the impact of a breach. Then, based on the incident's significance, the incident response leader will choose the appropriate path or play from the playbook.

Avoid unreported or underreported incidents by including reporting policies in regular company-wide security trainings. Everyone in the organization should know not to attempt to respond to an incident by themselves. After all, human error is the **number one** cause of data loss, so **normalize reporting over blaming**. Failure to report a problem is the problem – not the breach itself.

#5 Recovery

Recovery largely comes down to the business continuity and disaster recovery (BCDR) solutions that MSPs choose for themselves and their clients. Today's **cybersecurity landscape** demands more than just legacy backups to keep businesses open. Knowing how reliant SMBs have become on backups alone, bad actors are purposely deleting, encrypting, and holding them ransom to increase the likelihood of payment.

Fortunately, **modern BCDR solutions** give MSPs the tools and features necessary to recover from complex and sophisticated attacks. If your solution does not provide the following, you risk being unable to recover your backups, which could be fatal during a cyber incident.

MSPs should choose vendors that provide:

- → Automatic daily **backup integrity testing** and verification
- → Self-managed **disaster recovery** (DR) testing
- → Near-instant **virtualization** of workstations, servers, applications, and data in the cloud
- → **Anti-ransomware technology** so you never even consider paying the ransom

Developing Your Cybersecurity Playbook

Axcient has created an Incident Response Checklist to help cover your bases as you amass your cybersecurity playbook. Utilize this checklist and the information above as a jumping-off point and customize depending on industry, location, insurance policies, infrastructure, and feedback from your incident response team. This is merely the basics of a cybersecurity playbook, but it's enough to start getting you prepared for surviving the inevitable. Through discussions with your incident response team, quarterly updates and upgrades, and practice drills, you will develop a playbook that helps you sleep at night.

Incident Response Checklist

Executive/Business Perspective Responsible for critical decision making and communications.

ASSESS DAMAGE

- ◯ How widespread is the attack? Is it ongoing?
- ◯ Do you need to pull the plug on your tools or temporarily halt support?
- ◯ Delegate triaged outreach to affected customers
- ◯ Be aware of regulations and requirements (HIPAA, GDPR, etc.)

GET ON THE PHONE (JUST NOT WITH YOUR CLIENTS YET)

- ◯ Contact cybersecurity insurance provider and/or lawyer(s)
- ◯ Coordinate with (insurance-approved) IR provider
- ◯ Secure additional outside help/surge capacity
- ◯ Contact law enforcement (discretionary)

GET YOUR STORY STRAIGHT

- ◯ Determine how much to share and with who
- ◯ Coordinate with team re: communication scripts/ templates for both notifying and updating clients and responding to press inquiries
- ◯ Review communications with lawyer

UTILIZE YOUR TEAM

- ◯ Use your best technical staff to stop the bleeding Delegate keeping the lights on to other techs
- ◯ Have non-technical staff answering phones and responding to email
- ◯ Run damage control with key affected clients

Incident Response Checklist

Technical Perspective Responsible for containment, isolation and restoration.

LOCK DOWN YOUR ACCOUNTS AND TOOLS

- ◯ Audit for unusual tasks, scripts, policy changes, etc.
- ◯ Disable user accounts associated with abnormal/ malicious behavior; terminate active sessions
- ◯ Isolate any endpoints and other accounts associated with those users
- ◯ Minimize logging into affected systems using privileged credentials
- ◯ DO NOT shut down affected systems, change all passwords
- ◯ Ensure MFA is enabled on all accounts
- ◯ Confirm AV is enabled and updated, run deep scan
- ◯ Backup log files

LOCK DOWN AFFECTED CLIENTS

- ◯ Isolate affected client endpoints by taking them off the network
- ◯ Ensure backups are isolated/protected
- ◯ Minimize logging into affected systems using privileged credentials
- ◯ DO NOT shut down affected systems

NEXT STEPS AFTER ISOLATION

- ◯ Triage to determine further remediation priorities
- ◯ Strongly consider bringing in incident response specialist

Additional resources to become incident ready:

- Disaster Recovery Planning and Testing Best Practices Playbook
- BCDR Consolidiation: When to Think Cloud First
- x360Recover Direct-to-Cloud with Local Cache: Fast Recovery and No Pricey Appliance
- A Guide to Surviving a Total Ransomware Takedown

See how Axcient **x360Recover** provides comprehensive business continuity to reinforce your cybersecurity playbook **without the local appliance.** Using **Chain-Free technology,** Axcient allows MSPs to standardize, simplify management, and lower costs while providing best-in-class security with built-in, always-on features like **AutoVerify, Virtual Office,** and **AirGap.**

Sign Up for Your Free, 14-Day Trial Now!

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