INCIDENT RESPONSE PLANNING

WHY YOU NEED TO ESTABLISH A CLEAR CYBERSECURITY IR PLAN BEFORE IT'S TOO LATE.

5850 GRANITE PARKWAY, SUITE 720 | PLANO, TX 75024 | 214.297.2100 | WWW.AXXYS.COM | INFO@AXXYS.COM

Cyberattack rates are **climbing 47%** year over year.

Are you ready?

$4.88 million

The global average cost of a data breach.

58% higher costs

Companies without a structured and tested incident response plan pay nearly two-thirds more per breach than those with a formal plan.

$1.49 million saved

Organizations that rehearse their incident response at least twice a year slash breach costs by nearly one and a half million dollars.

258 days vs. 189 days

Companies without an incident response plan take nearly nine months to complete a breach lifecycle including detection, containment, eradication, recovery, and review. Those with a formal strategy cut that time to just over six months.

Did you know that 46% of small business owners report they have already experienced a cyberattack on their business? And 43% of all cyberattacks actually target small businesses because hackers see them as high-value targets with low security.

Being a small or midsize business doesn't make you immune to a cyberattack. In fact, your smaller size makes you more appealing to cybercriminals. The real question is, will your organization be ready to respond when it happens?

Limited IT staff, basic security tools, outdated technology, and overlooked vulnerabilities create easy entry points for attackers. They exploit those gaps to compromise business emails, steal credentials, deploy ransomware, and breach data, often without detection until the damage is already underway. What happens next depends on how prepared you are.

A well-designed incident response plan won't stop every attack. But it can control the fallout. It's the difference between returning to business as usual in days or spending months trying to recover.

What is IR Planning? It's more important than you realize.

Incident response planning is how you stay ahead of a security incident, not scramble to react after the fact. It's a structured, strategic approach built before a breach occurs. Everyone knows their role. Communication channels are clear. The response steps are documented and tested, so there's no guesswork when pressure hits. It combines preparation, risk assessments, scenario-based drills, and proven best practices. The goal is simple. To respond quickly, stay in control and limit the impact when an attack happens.

A strong incident response plan protects your business by:

Reducing Impact

When an attack happens, there's no time to figure things out on the fly. A solid plan aligns your internal team and external partners, giving everyone clear, role-specific steps to take. There are no confusion and no delays.

Keeping Operations Running

The faster you detect and contain a threat, the less downtime you face. A well-executed response can prevent a complete shutdown and keep critical parts of your business up and running.

Meeting Insurer Expectations

Most cyber insurers now expect you to have a documented incident response plan and often want to see evidence that you've tested it. Without it, getting a policy or having a claim honored can be a challenge.

Supporting Compliance

Privacy regulations and industry standards aren't just suggestions. Many require a formal response plan as part of your security program. Having one in place helps you stay audit ready.

Protecting Customer Trust

When something goes wrong, your response sets the tone. Fast, transparent customer communication can make the difference between maintaining confidence and losing hard-earned trust.

Strengthening Internal Awareness

Creating and testing your plan regularly keeps security top of mind for your team. It reinforces accountability and builds a culture of readiness across your organization.

SECURITY INCIDENTS CAN BE **INTENTIONAL OR ACCIDENTAL**

Some incidents start with a deliberate attack. Others result from simple mistakes by people with legitimate access and good intentions. Either way, the consequences can be devastating.

Ransomware

This form of malware locks or encrypts systems and data, demanding payment to restore access. It spreads quickly and can disable key functions in minutes, stopping operations cold.

Phishing and Social Engineering

Attackers impersonate trusted contacts through email, text, or phone to manipulate users into sharing credentials, transferring funds, or downloading malware. These attacks bypass systems by exploiting people.

DDoS Attacks

Distributed denial-of-service attacks flood systems with traffic, overwhelm the infrastructure, and cut off access to apps and services users rely on.

Insider Threats

Not all threats come from the outside. Whether intentional or due to poor judgment, like storing passwords in unsecured locations, authorized users can also put critical systems at risk.

Privilege Escalation

An attacker starts with limited access and then exploits system flaws to elevate their permissions. This can lead to control over sensitive data or entire networks.

Supply Chain Attacks

A trusted vendor with weak security can become the backdoor into your environment. These attacks introduce risk through third-party connections and compromised software.

Man-In-The-Middle (MITM) Attacks

These attacks intercept data in transit. The attacker commonly reads, changes, or redirects communication without either party realizing it happened.

LESSON:

Your incident response plan should continually address each threat's evolution as it becomes a more sophisticated risk.

CASE STUDY

FINANCIAL SERVICES CLIENT

IR Planning and Tabletop Exercise

Overview

A financial services client was required by their auditor to develop an Incident Response (IR) plan addressing a cyberattack scenario involving ransomware. The client also chose to create additional plans for other common cyber incidents including website defacement and business email compromise.

Client Challenge

The client's primary challenge was understanding the methodology for building valuable incident response plans and testing their effectiveness. To address this, Axxys was engaged to lead the information-gathering process and develop structured plan templates.

Axxys Solution Selected

Axxys delivered a set of three tailored IR plans covering:

- Ransomware
- Business Email Compromise
- Website Defacement

The Axxys Approach

We guided the client through a **structured seven-step** process to develop and document each plan. These steps ensure a comprehensive and repeatable response framework.

- **Preparation:** Ongoing improvement of incident response capabilities. This includes securing systems, networks, and applications, implementing employee awareness training, and conducting periodic tabletop exercises with the Incident Response Team (IRT).

- **Identification:** Confirming, classifying, and prioritizing suspected incidents to determine scope and impact.

- **Notification:** Alerting IRT members and key internal and external stakeholders and maintaining communication throughout the incident.

- **Containment:** Minimizing financial and reputational loss, preventing theft of information, and reducing service disruption. Initial communication with constituents and media is managed as needed.

- **Eradication:** Removing the threat from the environment.

- **Recovery:** Restoring systems and business operations quickly and securely, while implementing reputational repair measures and media updates if required.

- **Post-incident Activities:** Evaluating the overall response, identifying lessons learned, and incorporating improvements into future cyber defense and response plans.

Once each step was documented, Axxys built out the formal IR plans.

The next phase involved assembling the client's internal team alongside Axxys' security professionals. Together, they conducted a **tabletop exercise** to simulate incident scenarios. Axxys ensured that all roles were clearly defined and understood. And adjustments to the plans were made where necessary to reflect real-world conditions.

The tabletop exercise is scheduled and completed annually. Each year, the plans are updated to reflect changes in the client's business environment, evolving risk profile, and partner relationships.

Current Status

Today, the client continues to conduct annual tabletop exercises, with updates made regularly to keep IR plans aligned with business and risk changes. Most recently, a third-party auditor led the IR tabletop exercise without any participation from Axxys. This independent test demonstrated that the plans are solid on their own and can be followed effectively even when Axxys is not involved in the incident recovery.

In-House vs. Outsourced IR Response Teams. Which One is Better?

Even the best in-house IT teams are stretched thin. You're juggling infrastructure, support, patching, and upgrades. Then, an incident hits.

Most internal IR plans rely on limited tools, shared responsibilities, and documentation that may not be current or even accessible during a real attack. If that plan lives on the network and the network goes down or the file is inaccessible, you're flying blind.

An outsourced IR team gives you immediate access to specialists who work in this space full-time. They come equipped with advanced detection tools, deep threat intelligence, and the expertise that comes from regularly handling real-world attacks. They're not starting from scratch or scrambling to figure it out under pressure. They already know what to do and can hit the ground running.

It's not about replacing your internal team. It's about giving them backup when things go sideways. An experienced Managed Security Service Provider or MSSP can help you respond faster, recover smarter, and get back to business without turning your entire IT operation into a firefighting crew.

How a Security-Focused MSP Can Deliver the Best Results

Partnering with a generalist Managed Service Provider can help streamline your IT operations. But taking a generalist approach only goes so far when it comes to security. That’s where a security-focused specialist like a Managed Security Service Provider adds real value.

MSSPs are breach ready 24/7, 365. While MSPs handle daily IT management, MSSPs focus on threat detection, incident response planning and execution, and recovery. They don’t just create plans. They build systems that can spot the early signs of compromise and trigger a coordinated response before the damage spreads. They’re shaped by real-world incidents and regularly updated to reflect how attackers actually operate.

You also get tools designed from the ground up for security. MSSPs use purpose-built platforms to collect, compare, and act on threat data in real time. They don’t just review logs. They interpret behavior, flag anomalies, and respond fast. They don’t hand you a document and walk away. They test, refine, and stand by your business when it counts.

Most importantly, MSSPs treat incident response as a living process. As your environment changes, your plan evolves. It’s reviewed, stress-tested, and aligned with your risk profile. Not locked in an outdated static document.

Five Smart Questions to Ask an MSSP Before You Trust Them with Your IR Plan

Which cybersecurity frameworks guide your incident response planning?

Look for a Managed Security Service Provider that follows established frameworks like NIST (National Institute of Standards and Technology) or CIS controls v8 (Center for Internet Security's Critical Security Controls). These aren't just buzzwords. They are tested, widely accepted standards that ensure your response plan is built on a solid foundation. If a provider can clearly explain how their processes align with these frameworks, that's a strong signal that they take security seriously and follow industry best practices.

Do you include security services such as penetration testing or vulnerability assessments?

An MSSP that offers services like pen testing and vulnerability scans is better positioned to spot weak points before attackers do. These assessments directly inform a stronger incident response plan by highlighting the risks that need immediate attention. It also means the provider thinks proactively. They are not just waiting to react once something goes wrong.

Do you use the same security tools and processes to protect your own business that you recommend for your clients?

Their answer to this question will reveal a lot. A provider that uses the same tools and strategies internally as they offer to you shows they trust their own advice and stand behind what they sell. If they're not securing their business with the same resources, that is a red flag. You want a partner who uses what they sell.

How do you keep clients informed during a cybersecurity incident?

Clear, real-time communication is critical in the middle of an incident. The right partner should be able to walk you through their communication process. For example, who contacts you, how often, what kind of updates will you receive and how are decisions escalated? You don't want surprises or silence when the pressure is on. You need a team that communicates clearly and supports fast, informed decision-making throughout the incident.

How do you tailor your incident response planning to fit my business needs and risk profile?

The right partner should build your plan around your business, not just hand you a generic template. Look for a provider that takes time to understand your size, industry, infrastructure, technology stack, and specific risks. That includes evaluating your regulatory requirements, existing security posture, and operational needs. An incident response plan customized to your environment will help you respond faster, recover sooner, and limit the damage. If your MSSP cannot explain how they adapt their planning to fit your risk profile, they're not protecting your business effectively.

WHY MULTI-FACTOR AUTHENTICATION IS ALSO A MUST HAVE

Multi-factor authentication (MFA) is critical because it adds another layer of protection beyond simple passwords. Even strong passwords can be compromised through phishing, stolen credentials, or simple guessing.

MFA's requirement of two or more verification levels adds a critical barrier that prevents unauthorized access to systems and data. This added barrier helps prevent breaches before they happen and reduces the number of incidents your response team needs to deal with.

For incident response planning, MFA lowers the risk that attackers can move freely inside your network after an initial compromise. It limits their ability to escalate privileges, access sensitive systems, or steal critical data.

This front-line defense strengthens your overall security posture and gives your team a critical advantage in quickly containing and mitigating incidents.

THE AXXYS DIFFERENCE

WHAT MAKES AXXYS DIFFERENT?

Risk mitigation by certified security engineers.

Your security strategy is only as strong as the people behind it. Our Axxys team includes engineers with advanced certifications like CCNA Security, CISM, CISSP, CompTIA Security+, and CySA+. These credentials reflect hands-on expertise in identifying and reducing risk across complex environments.

Protected by ethical hackers.

Axxys certified ethical hackers (CEH) think like attackers so they can protect you from them. Using the same techniques threat actors use, they legally and ethically probe for weaknesses and help reinforce your systems before gaps become problems.

Around-the-clock threat detection with SIEM/SOC.

We use powerful SIEM/SOC technology to provide always-on threat monitoring and fast response. Our system pulls activity from across your network and applies real-time threat intelligence to flag and contain suspicious behavior before it spreads.

Custom security plans that fit your business.

There is no one-size-fits-all security plan. We design every Axxys Managed Security Plan to reflect your risk tolerance, compliance obligations, and operational goals. Whether you need a standalone solution or one that complements our managed IT services, we've got you covered.

A trusted MSSP partner.

As a designated Managed Security Service Provider, we're committed to leading with security top of mind and delivering enterprise-level protection. From proactive monitoring to incident response to compliance support, we help you stay secure and ahead of evolving threats.

Security awareness training that sticks.

Technology isn't your only line of defense. Your team is too. We deliver regularly scheduled security training that helps your staff recognize threats, follow best practices, and reduce human error because a well-informed team is harder to compromise.

Don’t have an incident response plan in place? Do you need to update an existing one? Have you already experienced an attack and need help immediately?

Contact an Axxys security specialist today.

GET STARTED