ActZero

Foundations for Incident Response Readiness

SMB Edition This guide can help small businesses prepare in advance for cybersecurity incidents, to reduce the impact and likelihood of data breaches.

CONTRIBUTORS:

Adam Mansour
Chief Security Officer

Will Ehgoetz
Manager, Threat Hunting

Immediate Steps: If You Think You're Experiencing an Incident Right Now

While most of this guide is designed to help small businesses prepare in advance for potential cybersecurity incidents, we didn't want to leave IT or business leaders out in the cold should they be searching for resources while an incident is underway. For those who are worried they're experiencing a cybersecurity event and aren't sure how to handle it, remember:

- Just as someone whose clothes have caught on fire should stop, drop, and roll before they even call 911, there are some immediate steps to take if the incident appears severe before calling in a cybersecurity emergency, aka external response teams.

Some signs that you're experiencing a severe enough incident to trigger the next three steps:

- A ransom note is present
- Firewall or IPS logs/alerts are showing signs of malicious IP connectivity or command and control signatures
- Users have informed IT of clicking on suspicious links
- Applications are not working or system performance is occupied by a scripting language like Python.

IMMEDIATE STEP 1: PULL THE PLUG

First thing's first: disconnect affected systems from the network. Swift containment and isolation of impacted systems are key. That's because breakout time--the time it takes for the bad guys to get full control over an entire SMB IT network after successfully compromising just a single machine—is extremely fast, often as quick as 15 minutes.

IMMEDIATE STEP 2: BREATHE

With that complete, take your hands from the keyboard for a moment, take a breath and think. If the organization does not yet have elite-level IR capabilities, you're likely going to need to call in help. Identify who you're going to call to lend emergency assistance.

IMMEDIATE STEP 3: COLLECT TRIAGE INFORMATION

The helpers will need information to triage and respond to your incident effectively, so begin by gathering and documenting the most important details about how your systems are behaving.

Information that outside IR specialists will ask for when you debrief them:

- The time of detection
- A brief description of the detection
- Usernames of affected accounts (if any)
- Host Names of the systems
- Local IP Address of the systems
- File extension names including full file paths
- Screenshots of threat behavior, ransom notes, etc

As you move through these steps, speed and decisiveness are of the essence. Taking swift steps to stop the attack chain can drastically reduce the risk of attackers causing the most costly damage. With that in mind, avoid overcomplicating things.

WHAT NOT TO DO:

- Don't ignore the red flags
- Don't try to attribute or conduct extensive threat research
- Don't try to build a detailed history to find the exact root cause
- Don't overcomplicate the debrief—time is of the essence

Thinking Ahead: Establishing a Sustainable IR Plan and Program

There's no better time to deal with a cybersecurity incident than before it has ever happened. Organizations who are just now recovering from an incident from which they were unprepared, learn this the hard way. And even those who have witnessed a competitor or similar organization in the news experience a difficult cyber incident should see that struggle as a wake-up call to think ahead about how prepared they are to respond to a similar intrusion.

While getting started can feel overwhelming and lock many small businesses into incident response (IR) analysis paralysis, we urge newcomers to keep the following IR tenants in mind:

- There is no such thing as a perfect incident response plan.
- An imperfect and simple plan is better than none at all. The goal should be to start small and incrementally improve over time.

Smart organizations can begin developing a simple plan and continue to iterate on it through a three-step cycle:

Prepare, Plan, Practice

1 Prepare

This is where an organization plans to make a plan. To prepare for the development of a new IR plan (or to improve an existing one) organizations must start with some basic but timely self-assessment.

Response planners should probe the current state of their organization by asking questions of themselves—about their team, their technology, processes, and business missions supported. They then should prepare a brief document that lays out what they've discovered by this quick look in the mirror. This document should be shared with IT and business leaders so that everyone can agree on priorities that will drive how the actual IR plan looks.

Self-assessments should help get a level set on the business, the assets at risk, and who's responsible for those assets:

KNOW YOUR BUSINESS:

Identify the key business processes that run the business

- Include front-of-the house processes that impact production of products, sales processes, and customer communication
- Also include critical back-office processes that keep the lights on, such as financial functions

KNOW YOUR ASSETS:

Map the technical capabilities that power those key business processes

- Mapped assets may include important database servers, and will almost certainly include your network directory infrastructure, such as Active Directory
- Similarly, don't forget important SaaS and cloud components of the asset portfolio, including Microsoft 365 infrastructure
- Comprehensive asset mapping is what mature organizations should strive for, but at very start just try to understand what are the critical assets that support processes that keep revenue streaming in
- Identify these critical assets by finding the most important systems, services, or data that if lost or otherwise interrupted, could lead to extreme business disruption, high costs to recover, or even going out of business
- These are systems or data that couldn't wait a few days to fix or reinstall, or that are proprietary in nature, such as the proverbial "secret sauce" recipe

KNOW WHO'S RESPONSIBLE:

Identify asset owners and operators for each documented asset

- Include both the main business stakeholder who depends on that asset, and the IT person in charge of administering it
- For smaller businesses without a lot of employees or lines of business, this should be fairly straightforward and will likely be the same person or people for most assets
- However, don't forget to list outside vendors in charge of assets—including SaaS and managed service providers--and important contacts at each
- Start with our template

With that self-knowledge in hand, organizations should list out the most immediate threats to the assets listed and consider those most likely to trigger security incidents. SMBs should keep it simple by identifying the most common scenarios impacting organizations like theirs, such as ransomware, account compromise, data theft, and malware outbreaks. The major threats enumerated here will stand as the main scenarios around which response procedures will be built. Organizations that need help identifying these scenarios would do well to learn a little bit about threat modeling to kick start this process.

Record all the knowledge you've dug up from this discovery process in a clear but simple document. Then use that to get an early sanity check from company leadership that these are, in fact, the priorities that should drive the cybersecurity IR plan. Running this document by the CEO before starting on the meat of the IR plan will save wheel spinning later on and increase the chances that the team can get solid buy-in from the highest levels of leadership planned responses to critical incidents that might seem extreme to those not informed of the risks. Making choices like these in the heat of an incident takes time that could make all the difference in preventing a minor incident from blowing up into a major one. By front-loading the decisions through early buy-in, those handling incidents on the ground will have the confidence to execute on IR plans immediately.

2 Plan

Develop a documented incident response plan by first creating action steps for the riskiest and most likely scenarios that threaten critical assets. These will typically be critical incidents. Subsequently consider other events that could also materially impact the business: these are high, medium, and low severity incidents.

For each scenario, detail the following:

IDENTIFICATION

This will detail how an incident becomes an incident. Identification of incidents most typically comes by way of cybersecurity detection and alerting technology, which triggers many response activities. But it should also include procedures for receiving user complaints or input that can act as a route for incident intake. This could include cases where a user's endpoint is displaying a ransomware ransom note or when a user suspects they may have clicked on a phishing message and they're now experiencing system abnormalities.

If the organization has minimal security detection and alerting capabilities, managed detection and response (MDR) services can help bolster their ability to find incidents earlier and more accurately.

EARLY RESPONSE AND REMEDIATION

Determine a list of what information and which logs need to be collected and what needs to be documented after an alert triggers for the particular scenario that's being planned for. For example, if an account compromise is suspected, the planned documentation list might be:

1. The time of detection
2. A brief description of the detection
3. Filenames and paths involved
4. Workstation names of impacted systems
5. Usernames of affected accounts
6. Source IP Addresses of Attackers

Develop a list of immediate steps to isolate and contain the threat before escalating and further investigating the alert. In the case of suspected account compromise, these steps might be:

1. Quarantine the asset: turn it off and unplug/disconnect from the network
2. Require user to reset passwords
3. Enable multi-factor authentication, if it is disabled
4. Investigate system logs associated with account to look for malicious access behavior
5. Determine if sensitive data is present and document the possibility of a breach

ESCALATION PROCEDURES

Decide what the technical triggers will be for unplugging or disabling a potentially compromised system. For example, if ransomware notes are found, that would trigger the endpoint from being removed from the network.

Determine a process and triggers for escalating to further investigation and help from an outside incident response team. Similarly, establish when authorities or regulatory bodies need to be contacted if a breach of personally identifiable information is suspected or confirmed.

Again, establishing these decisions clearly identifying escalation procedures here will help responders avoid pushback or hesitancy from stakeholders mid-incident who inevitably will argue, ‘Is it really necessary to shut this system down?’

COMMUNICATIONS PLAN

Decide who needs to be called internally and when they should be called as an incident escalates. This includes internal parties and external service provider contacts such as:

- Asset owners
- Help desk
- Service provider response teams
- Legal
- HR
- Corporate communications

Don’t just put in vague titles--include names, phone numbers, and email addresses for each contact that needs to be involved at various steps of escalation. Establish a communications and call tree contingency plan for cases when email or phone service has been disabled due to the incident. Make sure you also have a process/cadence by which this call tree is updated.

Additionally, consider coming up with an external communication plan for when and how external communication will be made to the following in the event of an incident or breach that impacts customers:

- Legal Departments
- Customers
- Journalists

Refer to our Breach Notification Rolodex to get insight into the external authorities an organization might need to contact in the event of a data breach.

CONTAINMENT AND RECOVERY

Document procedures for containment, bringing systems back online, recovering data, and remediating vulnerabilities/active threats so reinfection does not occur. Ideally an external response team can prove an invaluable partner in these clean-up steps.

Getting buy-in on these procedures is crucial. Once the draft of the plan is established, IT and security personnel should have business leaders and the CEO sign off on the plan, especially when it comes to drastic containment measures for critical incidents, such as taking revenue producing systems offline in certain scenarios.

Doing so will enable IT practitioners to act more quickly mid-incident without having to get someone to sign off on shutting down a key server or online service. This could make all the difference between an isolated infection and a massive incident that puts business viability on the line.

List the response action from your plan.

Be specific. You will practice these procedures, and the person doing them may change.

List the reasons you would respond this way.

The idea is to accept the business impact of the response, given the criteria, before that trigger occurs.

This makes action clear for the responder - if criteria met, initiate response procedure.

List potential disruption of the response action.

Include systems & teams impacted; how long they will be impacted; and the severity of the impact.

List the person and function responsible. Use the roles you established in your IR plan - as the specific person may change.

List the name / title of the approver. This conveys on whose authority the responder is acting. It helps avoid pushback.

Response Procedure	Trigger / Criteria	Business Impact	Execution	Approved By
Quarantine Workstation	A workstation is infected	Single user down 4 hours Low	Helpdesk	CIO
Password Reset Afflicted Users	A user profile is behaving anomalously	Multiple users down ~1 hour Low	Helpdesk	CIO
Password Reset Across Admins	An administrator profile is behaving anomalously; An administrator profile is no longer accessible by personnel;	All admin profiles down, including for enterprise software. Time & severity vary	IT Manager	CIO
Disconnect Critical Server from Internet (eg, Exchange)	A critical server is infected	Org-wide disruption Time & severity vary	Systems Admin	CEO & CIO CFO if financial systems hit
Disconnect Network Entirely	Multiple endpoints encrypted with ransomware	Org-wide disruption Time & severity vary	Disaster Recovery	CEO & Leadership Team

Click to Download File

3 Practice

The first draft of an incident response plan is just the very start of robust IR preparation. Practice and testing are crucial to understand whether the plan is any good and to see how quickly the organization can respond with the procedures as they're written. It's only by practicing the steps again and again while racing against the clock that an organization will know if it's actually prepared or not. Continuous practice is what truly defines a workable plan.

Practice the plan by running through some common scenarios. Start with the simulated communications and actions of a tabletop exercise. One thing to understand is that these days the most effective tabletop exercises aren't actually conducted at a boardroom table. Instead it is better for the simulation leader to run them via collaboration platforms like Slack and email, inline with how people do their work on a day-to-day basis.

For example, have a user kick off a practice session by sending a ransom note to the help desk with an explanation of what happened, and have everyone run through the steps that they'd take via email.

After running the tabletop exercise, organizations could also consider actually shutting down servers/services (a la Chaos Monkey) in more intensive technical simulations. However, SMBs will likely need the help of external providers with experience running these practice exercises to limit the possibility of incurring unnecessary business risk.

Also consider actual incidents to be the most valuable kind of practice. Don't neglect to run postmortem meetings to learn from incidents themselves by documenting what happened and using those lessons to update the incident response plans.

Practice helps identify gaps in controls and in the IR plan itself to give clues to improving the plan and also building resilience through better targeted cyber investments.

PUTTING IT ALL TOGETHER

Use the following chart to document the preparation, plan and practice stages.

Cybersecurity Scenario Detection and Response Tracker

Scenario	Detection	Alerting	Response	Time
For any incident requiring escalation, execute your Call Tree and engage your team				
I've been hacked and don't know how they got in	None	User Reported	Call ActZero @ 1.855.917.4981	2 Hours
I've been hacked and believe they have accessed sensitive data	RDP Logs	Anti-Virus	For disclosure in your state, check Breach Notification Rolodex	3 Days

Click to Download File

How MDR Helps: Partnering Throughout the Incident Response Lifecycle

Running through preparation, planning, and practice of an IR response plan may illustrate to many SMBs where they lack the kind of visibility and security controls they need to properly alert to the threats to their own critical assets. If you're a response planner thinking about your resilience and readiness to alert, let alone respond to an incident, run through the following checklists now:

People, Process & Technology Checklist	
Use SIEM to monitor logs from your Firewall, AV, or other security technology each day?	□
Use MDR or EUBA to search for behaviors that indicate an advanced attack, or zero-day attack?	□
Use Threat Intelligence to screen malicious connections and find threats before they are classified by Firewall or AV?	□
Use Vulnerability or Hygiene Scanning to run attack simulations on your network and endpoints?	□
Have dedicated staff to run these Incident Response Tests, and create new use cases, 24/7?	□
Leverage benchmarks to harden software in your environment from attack, like m365, AWS, Google Cloud, Windows, or MacOS?	□
Understand and comply with controls across various compliance frameworks, such as NIST 800-171, CMMC 2.0, ISO 27001, or other cybersecurity or privacy-focused frameworks?	□

Cybersecurity & Compliance Outcome Checklist	
Demonstrate adherence to cybersecurity best practices to your customers, partners, or board?	□
Secure unpatched (or, EOS) operating systems like Windows 7 or Windows Server 2008?	□
Conduct tests for security threats across various vectors (endpoint, network, cloud) and inform leadership of the results?	□
Articulate how your organization would detect, contain, and monitor a Ransomware outbreak, on the first day of your Windows Administrator's four-week vacation?	□
Respond if a customer informed you they were breached via an email from your domain?	□
Present logs from all systems to your cyber-insurance provider or forensic investigator if they needed to look for suspicious activity?	□
Red-team (penetration) tested outcomes like these?	□

Click to Download File

“MDR services provide remotely-delivered modern security operations center capabilities focused on quickly detecting, investigating and actively mitigating incidents[1]”

1. If you find yourself currently unable to fulfill these capabilities and/or lack the resources or expertise to meet them in the future, an MDR service may be able to strengthen your cybersecurity readiness (click here for a rubric to evaluate their capabilities).

2. MDRs are specialist firms you can use to deliver advanced cybersecurity functions. It’s a bit like renting parts of a SOC that an organization wasn’t likely to build itself, but which would be necessary to continuously protect the business.

3. It’s very normal for SMBs to discover through incident response planning that there are controls and response capabilities that they simply cannot fully cover with only internal staff and tooling in a cost effective manner. MDR can help them achieve the controls they need, and mitigate security risk in the right order.

4. In addition, if all of the response planning steps outlined here seem overwhelming, a great MDR provider can also provide supplementary help in devising an IR plan and testing it.

[1] 2021 Gartner Market Guide for Managed Detection and Response

Click here to engage ActZero for
Advanced Incident Response services.

Or, to see how our Managed Detection and Response service helps stop threats before they become breaches, check out our website or request a demo today.

About ActZero

ActZero's security platform leverages proprietary AI-based systems and full-stack visibility to detect, analyze, contain, and disrupt threats - all in one single, affordable, managed solution. No tools to buy and manage. No wasted time on needless alerts. And no more guessing where to focus your efforts. Just continuously hardened security, purpose-built for small and mid-sized businesses.

We actively partner with our customers to drive security engineering, increase internal efficiencies and effectiveness and, ultimately, build a mature cybersecurity posture.

ActZero

TORONTO
5045 South Service Road, Suite
300 Burlington, Ontario
L7L 5Y7

MENLO PARK
2882 Sand Hill Road, Suite 115
Menlo Park, California
94025

SEATTLE
Hawk Tower, 255 South King
Street, Suite 800 Seattle,
Washington 98104

in ActZero   ActZero   f ActZero.ai