redw
Advisors & CPAs

redw.com/cybersecurity

Cyber Incident Response Playbook: Preparing for the Inevitable

A guide to begin building organizational readiness for the modern threat landscape

Table of Contents

The Reality of Cyber Incidents

In today's digital business environment, ransomware has emerged as one of the most significant and costly threats facing organizations across all industries. This sophisticated malware doesn't just encrypt critical data—it cripples operations, damages reputations, and creates a lasting financial impact.

Modern ransomware attacks have evolved far beyond opportunistic encryption. Today's threat actors conduct thorough reconnaissance before striking, often maintaining unauthorized access for weeks or months before deploying their payload. Many employ "double extortion" tactics, threatening to release sensitive data publicly while simultaneously demanding payment for decryption keys.

The cybercrime ecosystem has professionalized with Ransomware-as-a-Service (RaaS) models, allowing even technically unsophisticated attackers to deploy enterprise-grade campaigns. This has contributed to the alarming statistics we're seeing: an organization's average time to identify a breach stretching to 292 days and to contain a breach, 287 days.

Perhaps most concerning is that 93% of organizations experience repeat incidents** after an initial breach. This cycle of recurring attacks demonstrates that most organizations fail to implement comprehensive changes to their security posture after an incident occurs.

Throughout this playbook, we'll show you how trusted cybersecurity resources can help you break this cycle through proper preparation, effective response, and strategic recovery.

$4.88 MILLION average cost of a data breach in 2024*

292 DAYS average time to identify a breach*

287 DAYS average time to contain a breach*

93% of organizations experience more than one breach**

$1 MILLION potential savings by involving law enforcement*

*IBM Cost of a Data Breach Report 2024 **CyberArk 2024 Identity Security Threat Landscape

Incident Readiness: Are You Prepared?

Self-Assessment

Answer each question “Yes” or “No”:

Y	N	
□	□	1. Do you have a documented incident response plan?
□	□	2. Have you tested your incident response plan in the last 12 months?
□	□	3. Is your backup process regularly tested?
□	□	4. Do you have cyber insurance?
□	□	5. Are your key stakeholders aware of their roles during an incident?
□	□	6. Do you have law enforcement contact information readily available?
□	□	7. Is multi-factor authentication enabled on all critical systems?
□	□	8. Do you have a communication plan for notifying customers/partners?
□	□	9. Have you identified your critical systems and data?
□	□	10. Does your staff receive regular security awareness training?

Total up your score and find the interpretation on the following pages.

“Yes” (1 point) or “No” (0 points)

________ Total Score

Scoring guide & Interpretation

Cyber-Resilient (9-10 points) - Your organization demonstrates excellent incident response preparation.

Your cybersecurity posture shows strong preparation for potential incidents. You've implemented core protective measures and have established proper response protocols. This level of readiness can significantly reduce both the likelihood and impact of a cyber incident, potentially saving millions in breach costs. To maintain this position, focus on regularly updating your incident response capabilities and testing them against evolving threats.

Next steps: Enhance your cybersecurity program with advanced threat-hunting capabilities. Consider a third-party validation of security controls.

Security-Conscious (6-8 points) - Your organization has established basic incident response foundations.

You've implemented several important security controls, but gaps remain in your incident response capabilities. While you've taken meaningful steps, the lacking elements could significantly impact your ability to respond efficiently during a crisis. Research shows that organizations with comprehensive response plans save an average of $2 million in breach costs compared to those without.

Next steps: Prioritize addressing gaps in your incident response plan. Ensure it's regularly tested with a third-party cybersecurity vendor.

Developing Security (3-5 points) - Your organization has critical gaps in incident response readiness.

Your current security posture leaves your organization vulnerable to significant disruption in the event of a cyber incident. With an average breach identification time of 292 days and containment time of 287 days across industries, your organization would likely face extended recovery periods and higher costs without addressing these gaps. The foundation exists, but substantial work is needed.

Next steps: Conduct a formal cybersecurity risk assessment and develop a prioritized roadmap to address critical vulnerabilities.

At-Risk (0-2 points) - Your organization requires immediate attention to incident response fundamentals.

Your organization faces substantial risk in the event of a cyber incident, with limited ability to identify, contain, or recover from an attack. With the average cost of a data breach reaching $4.88 million in 2024, your organization could face existential threats without immediate improvement. The lack of fundamental controls makes you an attractive target for threat actors seeking easy victims.

Next steps: Seek immediate assistance to establish basic security controls, beginning with multi-factor authentication and a basic incident response strategy.

No matter your score, REDW's cybersecurity experts can help enhance your security posture with tailored solutions. Scan the QR code to learn more.

Incident Response Planning

Before an Incident

Prevention

Effective cybersecurity focuses on preventing breaches before they occur. Most organizations that experience a breach become repeat targets, creating a cycle that persists because fundamental security gaps remain unaddressed.

Prevention requires understanding threat actor behavior. Cybercriminals typically operate opportunistically—looking for the easiest targets. By implementing strong preventative measures against common attack vectors, you can significantly reduce your risk profile and become a less attractive target in the digital landscape.

Implementation Checklist for Preventative Measures

□ **Multi-factor Authentication (MFA)**

Implement MFA on all critical systems and accounts. According to U.S. cybersecurity officials, this single control stops 80-90% of intrusion attempts by requiring something you know (password) and something you have (mobile device) to gain access.

□ **Administrative Account Management**

Maintain minimal admin accounts with unique credentials for each administrator. Avoid shared accounts, implement strict access controls, and regularly audit privileged access to prevent lateral movement.

□ **Software Installation Controls**

Restrict users' ability to install software on company devices. This prevents both accidental installation of malicious applications and blocks malware from automatically installing when it infiltrates a system.

□ **Security Awareness Training**

Conduct regular security training for all personnel, including executives and IT staff. Social engineering remains the primary attack vector, with recent major breaches occurring through help desk manipulation.

□ **Regular Risk Assessments**

Perform comprehensive security evaluations to identify vulnerabilities before attackers do. Knowing your weak points allows you to prioritize remediation efforts and allocate security resources effectively.

During an Incident

Respond, Don't React

When a cyber incident occurs, your immediate response determines whether you'll face a minor disruption or a catastrophic breach. While it might be tempting to "pull the cables" to stop an attack, hasty reactions often cause more harm than good.

Many ransomware variants include "logic bombs" that trigger destructive actions if improperly disrupted. Instead, a measured approach following established protocols ensures proper evidence preservation, effective containment, and ultimately faster recovery. Always review your cyber insurance policy requirements first, as failure to follow specified procedures could invalidate your coverage when you need it most.

Do's and Dont's During a Breach

DO...	DON'T.
Review cyber insurance policy immediately	Panic and pull cables
Contact law enforcement	Make hasty decisions
Activate your incident response team	Ignore legal requirements
Document everything	Destroy evidence
Follow established protocols	Neglect communication responsibilities

After an Incident

Navigating the Complex Recovery Path

The aftermath of a cyber incident presents a critical juncture for your organization. While 93% of organizations experience multiple breaches, your recovery approach can determine whether you become part of this statistic or break the cycle.

Every organization's recovery journey is unique, shaped by the specific nature of the breach, your industry, regulatory requirements, and business structure. However, all successful recoveries share one common element: thorough analysis and strategic improvement.

Key Recovery Considerations:

The path forward requires careful evaluation of several critical questions:

- What was the full extent of the breach, and have all affected systems been identified?
- Which security controls failed, and why weren't they sufficient?
- How effective was your incident response, and where were the gaps?
- What regulatory or compliance obligations must be addressed?
- How will you rebuild trust with customers, partners, and stakeholders?

Breaking the Cycle:

The difference between organizations that experience repeated breaches and those that effectively break the cycle often comes down to expert guidance during this critical phase. Recovery isn't simply about returning to normal operations—it's about emerging stronger and more resilient.

Trusted cybersecurity experts can provide the objectivity and specialized knowledge needed to transform an incident from a devastating setback into a catalyst for improved security. They help ensure that the lessons learned translate into effective preventative measures, completing the security cycle and significantly reducing your vulnerability to future attacks.

Contact REDW's cybersecurity team for a confidential post-incident consultation that can help transform your recovery into lasting resilience.

Incident Response Timeline

CRITICAL ACTIONS

FIRST 24 HOURS

IMMEDIATE RESPONSE

- Document the incident time, date, and initial observations
- Activate your incident response team using contacts below
- Preserve all evidence and logs
- Notify cyber insurance provider
- Assess initial scope of the breach
- Implement immediate containment measures

EVALUATE

24-72 HOURS

INVESTIGATION & CONTAINMENT

- Work with external resources to investigate root cause
- Expand containment to prevent lateral movement
- Prepare internal and external communications
- Document all findings and actions taken
- Evaluate regulatory reporting requirements
- Begin developing recovery strategy

INVESTIGATE

RECOVERY PHASE

RESTORATION & LESSONS LEARNED

- Test and verify systems before restoration
- Implement additional security controls
- Return to normal operations in prioritized order
- Document lessons learned
- Update incident response plan
- Conduct post-incident review with stakeholders

RECOVER

Key Contacts List

Role	Name	Contact Information	Alternate Contact
Incident Response Lead			
IT Security Contact			
Legal Counsel			
Executive Sponsor			
External Security Firm			

External Resources

Resource Type	Organization	Contact	When to Engage
Forensic Investigation			
Law Enforcement			
Cyber Insurance			

Post-Incident Documentation

This overview provides the basic structure for an initial incident response. For a comprehensive post-incident review, REDW recommends a facilitated session with all stakeholders to thoroughly analyze:

- Technical aspects of the incident
- Effectiveness of response procedures
- Communication effectiveness
- Resource adequacy
- Security control improvements

Contact REDW's cybersecurity team for assistance with conducting thorough post-incident reviews.

Cybersecurity Vendor Evaluation

Incident Response Partner Evaluation Matrix

Rate each potential vendor on a scale of 1 - 5, where 1 = poor, 5 = excellent. Multiply each score by its weight percentage, then sum all values.

Criteria	Weight	Vendor A __________	Vendor B __________	Vendor C __________	Notes
Experience with similar incidents	25%				Consider industry-specific experience
Response time guarantees	20%				Look for response times under 4 hours
Communication protocols	15%				Regular updates, clear escalation paths
Forensic capabilities	15%				Evidence preservation, analysis tools
Legal/regulatory knowledge	15%				Familiarity with your industry regulations
Post-incident support	10%				Long-term remediation assistance
TOTAL SCORE	**100%**				Higher score indicates better fit

Need help selecting the right incident response partner? REDW's cybersecurity experts can guide you through vendor selection and help establish a complete incident response program. Scan the QR code to contact us.

Essential Questions to Ask Potential Vendors

Document responses from your top vendor candidates:

Experience Questions:

Describe your experience handling incidents in our industry:______________________________

____

What percentage of your clients have experienced repeat incidents?______________________

How many similar-sized organizations do you currently support?________________________

Process Questions:

What is your typical workflow when responding to an incident?__________________________

____

How do you handle evidence preservation and chain of custody?_________________________

____

What communication cadence can we expect during an active incident?___________________

Integration Questions:

How would you integrate with our existing security tools?______________________________

What information do you need from us to prepare for potential incidents?________________

____

How do you coordinate with our internal teams during a response?______________________

____

Performance Questions:

What metrics do you use to measure successful incident response?______________________

Can you provide anonymized examples of response timelines?__________________________

____

What lessons has your team learned from recent incidents?___________________________

____

DECISION GUIDANCE

□ Clear leader based on evaluation:______________________________________

□ Need additional information (specify):__________________________________

□ Consider engaging multiple vendors for different capabilities: ________________

□ Recommend proceeding with:____

redw
Advisors & CPAs

redw.com/cybersecurity

About REDW Cybersecurity Services

Expert Protection for Your Digital Assets

REDW's cybersecurity consulting team brings decades of experience helping organizations identify, prepare for, and respond to cyber threats. Our comprehensive approach combines industry-leading expertise, practical solutions, and a deep understanding of your unique business needs.

Our Cybersecurity Services Include:

- Cybersecurity Scorecard
- Cybersecurity Awareness Training
- Business Process Risk Assessment
- Cybersecurity Risk Assessment (IT and NIST)
- Cybersecurity Policy & Procedure Development

Why Partner with REDW?

With over 70 years of business advisory experience, REDW understands that effective cybersecurity is not just about technology—it's about protecting your business operations, reputation, and bottom line. Our cybersecurity experts work alongside our accounting, advisory, and technology professionals to provide holistic protection for your organization.

Our remote-first team members and office locations in Albuquerque, Phoenix, Oklahoma City, and Salem allow us to serve clients across the United States with responsive, personalized service.

Ready to strengthen your cyber defenses?
Take the next step. Contact us today!

Visit **redw.com/cybersecurity** to learn more about our services and schedule a consultation with our experienced team.

Contact Our Cybersecurity Experts

Trisha Wilbrand
Senior Cybersecurity Consultant

Jennifer Moreno, CISA
IT & Cybersecurity Consultant