



CYBER INCIDENT DATA BREACH RESPONSE PLAN

PLAYBOOK

CYBER INCIDENT DATA BREACH RESPONSE PLAN

This playbook is designed for corporate organisations and startups of any size handling customer, employee, or financial data.

A data breach or cyber incident rarely announces itself politely; rather, it surfaces as a strange login, a locked file, a customer complaint, or a call from a stranger claiming to hold the data. *What happens in the hours that follow determines not just the technical outcome, but the legal exposure, financial cost, and trust a company retains with its customers and investors.* This playbook is designed for corporates and startups of any size that handle customer, employee, or financial data, and is built to be used in the moment; not just read and filed away. It walks through the response in the order a real incident actually demands:

What to do in the critical first 72 hours, which regulators must be notified and by when and how to preserve evidence so the investigation isn't compromised, which fraud patterns tend to follow a breach, and how escalation should flow internally so no one is left guessing who's in charge?

I. HOW TO IDENTIFY A CYBER SECURITY INCIDENT?

Not all security alerts indicate a current breach. Security teams frequently start by distinguishing between legitimate malicious activity and normal noise. An employee may be travelling, for instance, if they log in from a strange place. However, responders start to interpret atypical login activity as a possible compromise when it is followed by unexpected account behaviour, strange network connections, or efforts to access systems outside of that user's typical role.¹

The organisation's incident response plan (IRP) should be launched as soon as responders conclude they are handling an active event. Delaying action in the early stages of an incident while awaiting total confidence frequently provides attackers more time to increase their access, move laterally across the network, or steal confidential information.²

¹ Maryne Robin, *Incident Response in Practice: What Really Happens During the First 72 Hours of a Cybersecurity Incident*, Omega Systems (July 14, 2026), <https://omegasystemscorp.com/insights/blog/cybersecurity-incident-response-first-72-hours/>.

² Matthew Toldero, *Hit with a Cyberattack? What You Do in the First 72 Hours Could Save Your Business*, Constangy Cyber Advisor (Dec. 9, 2025),

II. PURPOSE & SCOPE

A cyber incident can take on various forms, such as a compromised computer system, an unauthorised funds transfer, an employee stealing data upon their departure, or even a data breach involving a third-party vendor with access to your organisation. Each of these scenarios does not require a separate strategy; this playbook employs a unified response for all of them.

This playbook outlines how the organisation will respond to any suspected or confirmed data breach or cyber incident³. This includes:

- *Unauthorised access to systems, networks, or data*
- *Ransomware, malware, or destructive attacks*
- *Data exfiltration (customer, employee, financial, IP)*
- *Business email compromise (BEC) or payment fraud*
- *Insider threats*
- *Breaches by third parties or vendors that affect your data*

III. INTERNAL ESCALATION STRUCTURE

An incident is only managed well when everyone knows their role before the crisis begins. The table below shows who is responsible for what during a cyber incident. This includes the person coordinating the response from start to finish, legal counsel managing notification requirements, and the executives with the authority to make crucial decisions. Defining these roles ahead of time ensures that no one has to figure out "who's in charge of what" under pressure.

TABLE- I⁴

<https://www.constangy.com/constangy-cyber-advisor/hit-with-a-cyberattack-what-you-do-in-the-first-72-hours-could-save-your-business>.

³ *The First 72 Hours: What CIRCIA Means for Firm Leaders*, Shield IT Networks (May 14, 2026),

<https://www.shielditnetworks.com/post/first-72-hours>.

⁴ Cyril Amarchand Mangaldas, *Cyber Incident Response* (2025),

<https://www.cyrilshroff.com/wp-content/uploads/2025/10/Cyber-Incident-Response-Handbook.pdf>.

ROLE	RESPONSIBILITY
Incident Response Lead (IRL)	Manages the incident from start to finish, coordinates the Incident Response Team, and is the main point of contact (POC)
Legal Counsel	Decides on notification duties, handles legal privilege, and communicates with regulators.
Executive Sponsor	Approves spending, resources, and major decisions (like ransom payments).
IT/Security	Handles technical containment, coordinates forensics, manages remediation; may involve an external forensics firm
HR	Deals with employee data incidents, handles insider threat cases, communicates internally with staff
Finance	Evaluates financial risk, coordinates with the insurer, manages fraud-related transaction issues

Board Committee	Informed according to governance rules, may need to approve disclosures for public companies,
------------------------	---

IV. FIRST 72 HOURS- RESPONSE TIMELINE

- ❖ **The First Six Hours** - A crucial initial step is to establish a well-defined chain of command, along with efficient procedures and governance.
- ❖ **The First Twelve Hours** - As additional information and proof become available, keep an open mind because anything can change. But be prepared to move fast.
- ❖ **First Twenty-Four to Thirty-Six hours** - Since notice rules and regulations usually take effect during this period, convey the most accurate picture you can.
- ❖ **And Continuing** - While the first 36 hours are crucial, the next steps to handle the situation will be prioritised based in large part on potential litigation expenses, regulatory fine risks, legal, consultant, and advisor fees, and lost customer revenues⁵.

The First Six Hours

It is vital to begin with a clear chain of command and effective governance from the start. The following are involved⁶:

- *Activation of the Incident Response Team – the members of IRL, IT/Security, Legal and the Executive Sponsor all have their tasks defined before being asked.*
- *Quarantine affected systems – isolate them without disconnecting them from the network unless they are causing damage; do not turn them off.*
- *Credential rotation and forced logout for compromised accounts.*
- *Reporting to CERT-In (in the case of India) – the clock begins counting from when the incident is identified, not when it is confirmed; needs to be done within 6 hours.*

⁵ Supra note 2.

⁶ Xiaokui Zhang et al., *Data Breach: Analysis, Countermeasures and Challenges*, 19 Int'l J. Info. & Computer Sec. 402 (2022).

- *Opening the master incident log – append-only, time-stamped log that records every decision made going forward.*

First Twelve Hours

With more information becoming available and as evidence is uncovered, stay flexible – everything could still change. A scenario that seemed limited to a phishing event after three hours may seem different after ten hours, when it becomes an actual exfiltration attempt. However, get ready to act fast:

- *Keep scoping – scope of the breach, what was accessed, what data was actually exfiltrated versus just touched, number of records/individuals compromised.*
- *Involve external breach counsel and a forensics company if not already involved in the discussion.*
- *Reach out to your cyber insurance provider – most policies include clauses about doing this early in the process; some even specify who can be hired for the job.*
- *Do not try to settle into one particular storyline. Initial assumptions are frequently incorrect⁷.*

First 24 to 36 Hours

As notification rules and regulations tend to kick in within this timeframe, provide the clearest picture that you have at hand:

- *The decision as to whether this is a reportable incident is made by the legal counsel — a matter of law, not technology.*
- *Start work on (not necessarily send out) a notification to regulators and customers, even if the investigation may not be completed yet — a phased/preliminary notification is fine, even expected.*
- *Brief the executives and the Board.*

⁷ Maxine Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 Ill. L. Rev. 803 (2021).

- *Identify what jurisdictions and industry regulators need to be notified, as this will determine when you have to start ticking the clock, whether that is GDPR's 72 hours, CERT-In's 6 hours, HIPAA's 60 days, and so forth.*⁸

And Beyond

While the initial 36 hours are critical, everything beyond that point is determined by litigation risk, the risk of a fine from the regulators, fees incurred from attorneys/legal/consulting advisors, and lost revenue:

- *Send notifications to the appropriate regulators and individuals within the proper timeframe.*
- *Contact law enforcement if there are criminal elements to the problem.*
- *Base resource allocation decisions on which is the bigger risk: litigation, fines, cost of remediation, or lost customers rather than assuming equal priority for all work streams.*
- *Begin the post-mortem analysis once the systems have been stabilised because that will be how the cost of this incident is measured, not whether it's fixed.*⁹

V. EVIDENCE PRESERVATION: STEP- BY- STEP

Evidence gathered within the first hours of the incident is what will eventually allow things to be proven to regulatory bodies, insurance companies, or even the courts. These guidelines outline the procedures that must be followed in order to gather the evidence in a professional manner, including setting up a chain of custody, safeguarding the site, and gathering volatile data while you still have the opportunity. Failing to perform these stages sequentially is one of the most common mistakes made during incident response procedures.¹⁰

⁸ G.A.P. Rodrigues et al., *Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded US Companies*, 16 *Future Internet* 201 (2024).

⁹ Chris Gilbert & Mercy Abiola Gilbert, *Impact of General Data Protection Regulation (GDPR) on Data Breach Response Strategies (DBRS)*, 9 *Int'l J. Rsch. & Innovation Soc. Sci.* 760, 760–84 (2025), <https://dx.doi.org/10.47772/IJRIS.2025.914MG0061>.

¹⁰ EC-Council University, *How Investigators Preserve Digital Evidence: A Cyber Forensics Guide for 2026*, ECCU Blog (May 14, 2026), <https://www.eccu.edu/blog/how-investigators-preserve-digital-evidence/>.

- **Step 1: Safeguard the area**

Devices must be physically restricted right away. Wireless signals are blocked by Faraday bags, making remote wiping impossible. When necessary, network wires are severed. The next step is logical isolation, which involves removing a device from the network without turning it off.

- **Step 2: List every source of evidence**

Potential sources of evidence include endpoints, servers, mobile devices, cloud accounts, and network logs. Before touching anything, investigators must make a thorough inventory.

- **Step 3: Before touching, document**

Before any data gathering starts, network diagrams, screenshots of active screens, and photos of the actual scene are taken. The state of the system at the time of discovery is proof in and of itself.

- **Step 4: First, gather volatile data**

Many investigations fail at this stage. RAM, running programs, and active network connections all contain volatile data. When a gadget runs out of power, it vanishes. Pulling the plug was once thought to be a safe technique. Since then, digital forensics has identified it as destructive. Active network sessions, ongoing process lists, and encryption keys are all stored in volatile memory. That doesn't withstand a shutdown. These days, investigators use specialised instruments to capture RAM snapshots from live systems before any power outages.

- **Step 5: Produce forensic pictures**

Instead of dealing with real evidence, investigators make bit-by-bit duplicates of storage devices. Hardware or software write blockers stop the imaging process from writing anything back to the source drive.

- **Step 6: Use hash values to confirm**

Following imaging, investigators use MD5 or SHA-256 to create cryptographic hashes of the original and the copy. The image is identical to the source when the hash values match. Any future modifications to the hash indicate manipulation. For admissibility in court, this process cannot be compromised.

- **Step 7: Safely store and label**

Case numbers, collection dates, and investigator identities are labelled on evidence. Access to storage must be restricted. Every subsequent interaction is documented in digital chain-of-custody records.

VI. FRAUD INDICATORS TO BE AWARE OF

Some things to look out for during and after an attack that indicate ongoing financial fraud or future attacks include:¹¹

BEC fraud indicators: sudden change to vendor banking information, urgency around wire transfer payments, executive impersonation email with slight typos on the domain (e.g., compnay.com), requests to deviate from standard approval process.

Account takeover indicators: login activity from unusual geographic locations and time zones, MFA fatigue attacks (multiple push notification attacks), password reset requests without the user's consent.

Post-breach fraud: phishing campaign targeting your clients using stolen information ("Your account has been breached, click here to protect yourself"); impersonation phone calls claiming to be customer service with correct details; credential stuffing attacks using passwords leaked in the attack.

Fraud by third parties/vendors: spoofing invoice and payment requests from vendor's genuine email address, unexpected change to vendor payment details without calling the contact as usual, fraud occurring through your partner's system rather than yours.

Insider threats indicators: unusual access activity prior to termination or resignation, massive amount of data downloaded unrelated to job responsibilities, access to systems outside usual working hours and/or job description.

VII. CONCLUSION

A cyber attack not only challenges technology but also tests the organisation to determine if they had prior knowledge about leadership, deadlines, and how to ensure that evidence is preserved for regulatory or legal purposes in the future. The initial six hours shape the circumstances. The

¹¹ Abnormal AI, *13 Red Flags and Identifiers of a BEC Attack Every Security Team Should Know* (Mar. 15, 2026), <https://abnormal.ai/learning/bec-attack-identifiers>.

next thirty hours determine the extent of legal responsibility. However, none of this will be effective if we address it only spontaneously during the crisis. The organisations that come out of an attack with their credibility preserved are those that have preemptively determined the answers to all the difficult questions: Who has authority, who is responsible for making decisions, who communicates with regulators, and what must we protect before starting the cleanup? That is precisely the purpose of this playbook. Think of this as a dynamic process, not a static exercise. Regulations change, attack tactics get revised, and the individuals listed on the escalation chart move on.¹²

¹² Cheyenne Harden, *Cyber Breach Response: What the First 72 Hours Look Like*, Cyber Protect LLC (May 1, 2026), <https://www.cyberprotectllc.com/cyber-breach-response-first-72-hours>.



Fractional General Council

A-9, Block A, Sector 68, Noida,
Basi Bahuddin Nagar, Uttar Pradesh 201309

www.fracgc.in

contact@fracgc.in

[+91 83770 09673](tel:+918377009673)
