The First 4 Hours Battle-Card

Two pages. One for an infrastructure incident. One for a vulnerability disclosure. Designed to print and laminate.

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-09-14

Contents

The First 4 Hours Battle-Card **1**

Path A — Infrastructure Incident **2**
- First 15 minutes . . . 2
- Next hour . . . 2
- Do not touch . . . 2
- Regulatory clocks at a glance . . . 3

Path B — Product Vulnerability Disclosure **4**
- First 15 minutes . . . 4
- Next hour . . . 4
- Do not touch . . . 5
- Regulatory clocks at a glance (vendor-side) . . . 5

Five Standards Worth Knowing By Name **6**

Want the Full Triage? **6**

About This Guide **7**

The First 4 Hours Battle-Card

A printable, laminate-on-the-wall reference for the first hours of a real security incident. Two paths. One for your infrastructure being compromised. One for a vulnerability report against a product you ship. Both pages share the same structure: what to do in the first 15 minutes, what to do in the next hour, what to avoid, which clocks may already be running.

Reading this during an actual incident? Scroll to the page that matches your situation. Take a slow breath. Work the list in order. Do not skip the “avoid” section.

Path A — Infrastructure Incident

Your network, accounts, endpoints, or servers have been compromised, or you suspect they have.

First 15 minutes

1. **Note the time.** Several reporting clocks begin at awareness, not at the moment of compromise. Record the timestamp where you cannot lose it.
2. **Name one decision-maker.** Designate a single incident commander. One person whose call settles all questions for the next four hours. Write the name down where the team can see it.
3. **Get to a clean channel.** Move incident-response communication off any system that may be compromised. Use phones, a separate messaging app, or a known-clean machine.
4. **Network-isolate, do not power off.** Pull the affected hosts off the network. They cannot reach attacker infrastructure that way. Leave them running. Powering off destroys volatile evidence in memory.
5. **Call your cyber-insurance carrier.** Most policies require notification within a tight window of awareness. Many carriers have approved incident-response vendors they will pay for directly. Calling them first is often the cheapest move.

Next hour

6. **Engage qualified counsel.** Counsel typically must clear external communications. Counsel may also invoke attorney-client privilege over the response. Engage by phone, on the clean channel.
7. **Engage a forensics or incident-response firm.** No retainer? Your insurance carrier or counsel can usually source one within an hour.
8. **Map the apparent scope.** Identify which hosts, accounts, segments, and customer tenants are affected. This is what makes containment and notification decisions possible.
9. **Classify the data exposure.** Confirm what categories of data may have been accessed. Personally-identifiable information. Protected health information. Payment data. Intellectual property. Sensitivity drives reporting clocks.
10. **Preserve before you act.** Capture disk images and volatile memory before any action that changes machine state. Forensics teams cannot rebuild a timeline from a wiped machine.
11. **Identify regulatory category.** Public company? European Union "essential" or "important" entity? Critical-infrastructure operator? Regulated healthcare or financial? Each triggers different statutory clocks (see below).
12. **Confirm backups are usable and offline.** Online backups are commonly encrypted alongside production in ransomware events. The right question: is it recoverable from offline? Not just: do we have a backup?

Do not touch

- **Do not reboot, wipe, or reimage affected systems** before a forensics image is captured.

- **Do not pay any ransom** without first consulting counsel and your cyber-insurance carrier. Payment may break sanctions law (for example, the US Office of Foreign Assets Control list). Many policies also require carrier approval first.
- **Do not post about the incident publicly** until counsel and communications have signed off. Even if a public statement feels urgent.
- **Do not delete logs, suspicious files, or attacker tooling.** Preserve them in place where possible.
- **Do not contact the attacker yourself.** Not to negotiate, not for any reason. Specialist negotiators exist for a reason.
- **Do not assume a single host is the only one.** Lateral movement is the rule. Not the exception.

Regulatory clocks at a glance

Window	Trigger	Notes
24 hours	EU NIS2 Article 23 early warning, if you are an EU essential or important entity	Full notification within 72 hours; final report within one month
72 hours	US Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), if you operate US critical infrastructure	Ransom-payment reporting due within 24 hours
72 hours	EU General Data Protection Regulation Article 33, if European Union residents' personal data is affected	Notification to the lead supervisory authority
4 business days	US Securities and Exchange Commission Form 8-K Item 1.05, if you are a US public company and the incident is material	Clock starts from the materiality determination, not from awareness
60 days	US Health Insurance Portability and Accountability Act breach-notification rule, if protected health information is affected	Individual and Department of Health and Human Services notification
varies	US state breach-notification laws	All 50 states have a statute, with windows of 15 to 90 days. Confirm with counsel for the affected residents' state of residence.

Path B — Product Vulnerability Disclosure

Someone outside your organisation has reported a vulnerability in a product you ship.

First 15 minutes

1. **Note the time of receipt.** The European Union Cyber Resilience Act (CRA) reporting clock for actively-exploited vulnerabilities starts at awareness. Record the timestamp.
2. **Funnel the report into one channel.** All reports go to one tracked inbox (typically `security@`). Did the report arrive elsewhere: social media, customer support, a personal email? Copy it to the tracked inbox now. Reply asking the reporter to use that channel going forward.
3. **Acknowledge the reporter within 24 hours.** Even a one-line reply protects the embargo and the relationship. Example: "We received your report on [date]. We are reviewing and will respond by [date]."
4. **Name a single response owner.** No Product Security Incident Response Team? Designate one person as the owner for this report.
5. **Open a tracking ticket.** One ticket per report. Record the timestamp, the channel, the reporter's name and contact, the affected product, and the claimed severity.

Next hour

6. **Confirm whether the report is real.** Try to reproduce the vulnerability in a test environment. Confirming before acting avoids false alarms and dismissed real issues alike.
7. **Score it yourself with the Common Vulnerability Scoring System.** Use version 3.1 or version 4. The reporter's severity claim is a starting point, not the final scoring.
8. **Determine where the affected product is deployed.** European Union customer? Cyber Resilience Act applies (in force since 11 September 2026). Public-company customer? Their SEC obligations may indirectly affect your timeline.
9. **Confirm whether active exploitation is occurring.** Confirmed exploitation triggers the 24-hour Cyber Resilience Act early-warning clock. It also shortens embargo tolerance.
10. **Set the embargo in writing.** Reply to the reporter with the proposed disclosure date. Typically 90 days from acknowledgement. Sometimes 45 days for actively-exploited issues. A documented embargo protects both sides.
11. **Start the advisory draft.** Use the Common Security Advisory Framework (CSAF) format if you publish machine-readable advisories. Draft the human-readable advisory in parallel.
12. **Submit a Common Vulnerabilities and Exposures (CVE) identifier request.** Submit to your CVE Numbering Authority through the standard channel. The identifier should be ready when the fix lands.

Do not touch

- **Do not publicly disclose the vulnerability** before coordinating with the reporter. And for products in European Union scope since 11 September 2026: before filing the Cyber Resilience Act early-warning notification.
- **Do not threaten or pursue legal action against a good-faith security researcher.** This damages your reputation. It also chills future reports.
- **Do not deploy a silent fix and hope no one notices.** A silent fix creates a worse problem when independent researchers find it later. Pair every fix with an advisory.
- **Do not request a CVE number publicly** (for example, on social media). Submit to your CVE Numbering Authority through the standard channel.
- **Do not promise a fix timeline you cannot keep.** Underpromise and overdeliver. The reporter's trust matters.
- **Do not assume "we are too small for the Cyber Resilience Act."** The Cyber Resilience Act applies to any manufacturer placing products with digital elements on the European Union market. Carve-outs for non-commercial open-source are very limited.

Regulatory clocks at a glance (vendor-side)

Window	Trigger	Notes
24 hours	EU Cyber Resilience Act Article 14 early warning, for actively-exploited vulnerabilities in products with EU customers	Reporting obligations have applied since 11 September 2026. Submit to the EU Agency for Cybersecurity (ENISA) single reporting platform and the relevant national Computer Security Incident Response Team.
72 hours	EU Cyber Resilience Act Article 14 full notification	Follow-on detail to the 24-hour early warning
14 days / 1 month	EU Cyber Resilience Act Article 14 final report	14 days after a corrective measure (fix) is available, for an actively-exploited vulnerability; within one month of the 72-hour notification, for a severe incident
24 / 72 hours	EU NIS2 Article 23, if your organisation is an essential or important entity in its own right	Separate from the Cyber Resilience Act vendor reporting
4 business days	US Securities and Exchange Commission Form 8-K Item 1.05, if you are a US public company and the matter becomes a material cybersecurity incident	Coordinate with counsel
embargo	Coordinated disclosure with the reporter	Typically 90 days, sometimes 45 days for active exploitation. Set in writing.

Five Standards Worth Knowing By Name

These are the standards the recommendations above are drawn from. Knowing the names, not the contents, is enough for the first four hours.

1. **National Institute of Standards and Technology (NIST) Special Publication 800-61** (Computer Security Incident Handling Guide). The most widely-cited US framework for infrastructure incident response. Free.
2. **International Organization for Standardization (ISO)/IEC 30111** (Vulnerability Handling Processes) and **ISO/IEC 29147** (Vulnerability Disclosure). The international standards for vendor-side response to security reports. Worth a single read.
3. **FIRST PSIRT Services Framework** (Forum of Incident Response and Security Teams). Defines the eighteen services a Product Security Incident Response Team is expected to provide. Free.
4. **Common Vulnerability Scoring System (CVSS) v3.1 and v4.** The de facto severity-scoring system for vulnerabilities. Free calculator at first.org.
5. **Common Security Advisory Framework (CSAF) v2.0.** The machine-readable format for security advisories. Grows in relevance as the Cyber Resilience Act reporting platform comes online.

Want the Full Triage?

The free First 4 Hours Incident Triage at *first4hours.sylvanassurance.com* asks nine questions about your current situation and returns:

- A triage band (Stable / Elevated / Acute / Critical) with a phase breakdown.
- A list of the regulatory clocks that may already be running, based on your answers.
- A path-specific “do not touch” list.
- A prioritised next-action list.

It runs entirely in your browser. Your answers are never transmitted.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience translated into plain-language guidance for small business owners.

It provides **general guidance and recommended practices**. It is **not** legal advice. Every recommendation is **optional** - a widely accepted way to reduce a common risk. Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with the First 4 Hours Incident Response.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here

Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-first-4-hours

Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/first-4-hours