



The First Hour.

What your company does in the first sixty minutes of a cyber incident.



BASED ON NIST SP 800-61 REV. 3 AND THE CISA #STOPRANSOMWARE GUIDE

EDITION FOR THE PEOPLE WHO DECIDE · ENGLISH



Why the first hour decides the cost of the months that follow

This document was requested on the Zamak website by someone at your company, or it reached you forwarded. It describes what a company does in the first hour of a cyber incident and why that hour decides how long the operation stays down, how much it pays and what will be said about it. It was written to be read by the people who decide, not only by the people who operate, and it can be forwarded without any additional context.

A ransomware attack rarely starts at the moment it is noticed. The intrusion comes before the alert, often through a stolen credential or a phishing email; the attacker moves through the network, copies data and only then encrypts the systems. When the alert arrives, the clock that matters is the response clock.

In that hour, three things are decided at once: how long the operation stays down, how much the company pays (in ransom, in recovery, in fines and in contracts) and what will be said about it by customers, press and regulators.

CISA, the United States cybersecurity agency, recommends identifying the affected systems and isolating them immediately as the first step, powering a device down only when it cannot be disconnected from the network. NIST, in SP 800-61 Rev. 3 (2025), treats incident response as part of the company's risk management, not as an isolated IT task. This playbook applies both in business language.

The first hour is not technical. It is a matter of decision.

How to use this document

TODAY

Read it once, calmly. Name who does what on page 4 and fill in the four numbers on page 5.

NEXT TO THE PHONE

Print it, cut out the card on page 7 and leave it with the person who decides. On the day, nobody searches for a file.

ON THE DAY OF THE INCIDENT

Open page 3 and follow the minute column. One decision per line, none skipped.

AFTERWARDS

Take page 6 to leadership: five questions and a list to close before the next time.



The sixty minutes, step by step

One decision per line. The clock starts when someone notices something is wrong, not when the problem is confirmed.

MINUTE	WHAT HAPPENS	WHO	WHY
0-5	Disconnect, do not wipe Disconnect the affected systems from the network, without wiping or reformatting anything. Power down only if you cannot disconnect.	Whoever is in front of the system, with the IT and security partner	Stops the spread and preserves what the investigation will need.
5-15	Declare the incident One lead, one communication channel outside the affected systems, one log with the time of every decision.	Executive leadership	Without an owner, each area decides alone and the company loses time and evidence.
15-30	Preserve Confirm the backups are isolated and intact; freeze images of the affected systems; nothing is rebooted to see if it comes back.	IT and security partner	Rebooting can destroy evidence the investigation needs.
30-45	Call the four numbers IT and security partner, cyber insurer, legal counsel and the competent authority.	Executive leadership and finance	Policies typically require prompt notice; data protection laws set deadlines; the authority guides and records.
45-55	One voice Leadership defines what the company says to employees and customers; nobody speculates or posts on social media.	Leadership and communications	Reputation is decided by the consistency of what is said in the first hours.
55-60	Decide the next hour Known scope, continuity plan activated, who talks to customers and when.	Everyone accountable, in a short meeting	Turns reaction into a plan and gives the company back control of the clock.



Who does what

Name them today. On the day, nobody has time to discuss roles. Every role has an owner and a backup.

ROLE	ACCOUNTABLE FOR	OWNER · BACKUP
Who decides	Declares the incident, authorizes spending and shutdowns, speaks for the company. Usually the owner, the CEO or the managing director.	OWNER BACKUP
Who contains	Isolates, preserves evidence and leads recovery. The IT and security partner, with the internal IT team where there is one.	OWNER BACKUP
Who notifies	Engages the insurer, legal counsel and the authority; tracks legal notification deadlines. Legal and finance.	OWNER BACKUP
Who communicates	Writes and delivers the single message to employees and customers. Communications or HR, under the word of the person who decides.	OWNER BACKUP
Who records	Logs the time of every decision and every contact, on paper or in a channel outside the affected systems. Anyone trusted.	OWNER BACKUP

The hour is going well when

- ◆ There is one owner and everyone knows who it is.
- ◆ The affected systems are off the network and nobody has rebooted anything.
- ◆ The four numbers have been called and the time of each call is written down.

The hour is going badly when

- ◆ Three people are deciding different things at the same time.
- ◆ Someone rebooted or reformatted a system to see if it comes back.
- ◆ A customer heard about the incident before leadership did.



What never to do

- X Pay on impulse.** CISA and the FBI do not recommend paying a ransom: payment does not ensure the data is decrypted or that it will not be leaked.
- X Reboot or reformat to see if it comes back.** It destroys evidence and can trigger the next phase of the attack.
- X Delete suspicious logs and emails.** They are the evidence the investigation and the insurer will need.
- X Post before you know.** A public message without a known scope becomes a headline and does not come back.
- X Negotiate alone.** Any contact with the attacker goes through legal counsel and the insurer.

The four numbers

Fill them in today and keep them next to the phone of the person who decides.

IT and security partner

The one who isolates, preserves and recovers. If the answer is we will figure it out when it happens, this is the first number to solve.

COMPANY

.....

NAME

.....

24H PHONE

.....

Cyber insurer

The policy usually sets a notice deadline and names the response vendors. Check yours.

INSURER

.....

POLICY NO.

.....

CLAIMS PHONE

.....

NOTICE DEADLINE

.....

Legal counsel

Data protection laws, such as state laws in the United States and the LGPD in Brazil, set notification deadlines and obligations.

FIRM

.....

NAME

.....

PHONE

.....

Competent authority

In the United States, the FBI takes reports through IC3; in Brazil, the specialized cybercrime police unit.

AGENCY

.....

CHANNEL

.....

PHONE

.....

The one-page version for leadership

Five questions leadership can ask today, before any incident, and what a good answer looks like.

-
- 1 Who decides in the first hour, and who decides if that person is not available?
Two names, in writing, known to the whole leadership.

 - 2 How many hours can the operation stay down before it becomes irreversible loss or news?
One number per critical area, and a continuity plan for each.

 - 3 Where is the backup, is it isolated from the network, and when was the last recovery actually tested?
An immutable copy, out of the attacker's reach, with the date of the last recovery test.

 - 4 Who speaks for the company, and what do they say, in the first hours?
One spokesperson and one base message approved before it is needed.

 - 5 Which contracts, policies and laws require notice, and how quickly?
A list with the deadlines, reviewed by legal and finance.

Before the next time

- | | |
|--|---|
| ☐ Immutable backup, isolated from the network, with tested and dated recovery | ☐ Detection and response on every endpoint, not just antivirus |
| ☐ Multi-factor authentication on email, remote access and administration | ☐ Response plan with names, backups and a channel outside the systems |
| ☐ Cyber policy read: notice deadlines and required vendors | ☐ One rehearsal a year: one hour, at the table, with the people who decide |

Pocket card

Cut it out and keep it next to the phone of the person who decides.



The First Hour.



0 - 5	5 - 15	15 - 30	30 - 45	45 - 55	55 - 60
Disconnect, do not wipe	Declare the incident	Preserve	Call the four numbers	One voice	Decide the next hour

Four numbers: IT and security partner · insurer · legal counsel · authority

How Zamak prepares the first hour

For the companies Zamak serves, the first hour starts before the incident: detection and response on every endpoint, immutable backup copies with recovery that can be tested, and service in English, Portuguese and Spanish, within the scope each company engages. For companies with their own IT team, Zamak works alongside it as an operations and security center.

Serving companies that cannot stop. Microsoft Solutions Partner and Addee (N-able) Elite Group, operating with defense and backup tools whose manufacturers are certified in SOC 2 Type II, ISO 27001, HIPAA and PCI-DSS.

→ Talk to a Zamak specialist

<https://www.zamakt.com/en/appointment>

→ Calculate what one hour of downtime costs your operation

<https://www.zamakt.com/en/tools/downtime-calculator>

→ Share this playbook with your leadership

<https://www.zamakt.com/en/resources/first-hour>

Sources: [NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management \(April 2025\)](#) · [CISA and FBI, #StopRansomware Guide and Ransomware Response Checklist](#)

Educational material from Zamak Technologies. It does not replace an incident response plan designed for your company, work Zamak carries out when the service is engaged.



Saving time, money & business reputation.

Sixty minutes. Six
decisions. One voice.



FREE PLAYBOOK · ENGLISH · PORTUGUÊS · ESPAÑOL

ZAMAKT.COM/EN/RESOURCES/FIRST-HOUR