FREE GUIDE · KEEP WHERE YOUR TEAM CAN FIND IT

Ransomware First-Response Guide

The first hours of a ransomware attack decide how much can be saved. This is what to do, what not to do, and the recovery paths that avoid paying, from the Australian team that rebuilds data other methods have written off.

Do this first

- ✓ **Isolate, but keep the power on.**
  Unplug the network cable or turn off Wi-Fi on affected machines. Do not shut them down: memory and running state can matter to recovery.
- ✓ **Keep the encrypted files and every ransom note.**
  Partially encrypted files are often recoverable. Deleting them removes that option permanently.
- ✓ **Take your backups offline now.**
  Attackers routinely encrypt or delete every backup they can reach. Disconnect them before anything else does.
- ✓ **Get help before you change anything.**
  The first moves decide what can be saved. Call a responder before touching the affected systems.
- ✓ **Start a timeline.**
  Note what happened and when: first signs, systems affected, actions taken. Plain notes on paper are fine. They matter for insurance, reporting, and recovery.

Not yet, or not at all

- ✗ **Don't wipe, re-image or rebuild yet.**
  Rebuilding destroys the evidence and, with it, often the data. Recovery works on what is left behind.
- ✗ **Don't run removal or "cleanup" tools over the top.**
  Cleanup tools overwrite exactly the material a recovery works from.
- ✗ **Don't restore backups into the compromised environment.**
  Confirm backups are intact and clean, then restore into a known-good environment, never over the top.
- ✗ **Don't pay the ransom yet.**
  You may not need to. Payment funds the offender, guarantees nothing, and in Australia triggers its own reporting obligation.
- ✗ **Don't assume the ransom note is telling the truth.**
  Data-theft claims are frequently a bluff. Assess them rather than accept them.

Under attack right now?

Australian incident response, answered by a real person 24/7. The sooner you call, the more we can bring back.

1300 004 766

BEFORE ANYONE PAYS

The recovery ladder: work it in this order

Payment is not step one. It is what you consider when every rung below has genuinely been exhausted, and even then it funds the offender and guarantees nothing. Most businesses have more options than they think.

1 **Clean, verified backups**
Offline or immutable copies, checked before restoring, restored into a clean environment.

2 **Shadow copies and snapshots**
If the attack did not delete them, volume shadow copies or SAN snapshots can bring systems back quickly.

3 **Partial-encryption recovery**
Many strains scramble only the front of large files for speed. The untouched data can be located, carved and rebuilt without the attacker's key. Often the path that saves the day when backups are gone.

4 **A public decryptor**
On the rare occasion keys leak or the strain has a known flaw. Check nomoreransom.org, but do not plan around it.

5 **Rebuild from source systems**
Where the data still exists elsewhere: line-of-business SaaS, bank records, supplier and customer copies.

Your obligations in Australia

Notifiable Data Breaches scheme
If personal information was accessed and serious harm is likely, assess promptly (within 30 days at the outside) and notify the OAIC and affected people. Unauthorised access can be enough.

Cyber Security Act 2024
If a ransom is paid, businesses over $3 million turnover must report the payment within 72 hours.

ReportCyber
Report the incident to the ASD's ACSC via ReportCyber, whether or not you pay.

General guidance, not legal advice. Seek your own counsel.

About IronSights

IronSights is a Sydney cyber security firm serving businesses Australia-wide: incident response, ransomware data recovery, managed security, and penetration testing. ISO 27001 and ISO 9001 certified. This guide, and the detailed recovery methodology behind it, live at ironsights.com.au/ransomware-data-recovery. Share the guide freely; it may save someone a very bad week.