

Ransomware Incident Response: Why Paying the Ransom Is a Failure of Preparation - blueAPACHE

Canonical: <https://www.blueapache.com/blog/ransomware-incident-response-why-paying-the-ransom-is-a-failure-of-preparation>

Details:

For our vCISO, the early months of 2026 have sharpened focus on the disciplines that ultimately decide whether a ransomware incident becomes disruption or disaster: Incident Response (IR), Disaster Recovery (DR) and Business Continuity Planning (BCP). These areas are often grouped together, but in practice they fail for very different reasons. That focus was reinforced by a recent iNews article examining Australian organisations paying ransoms to regain access to their systems. In effect, these payments do more than restore operations. They directly fund organised cybercrime. When Australia's largest organisations pay ransomware demands, the issue stops being technical and becomes a failure of leadership, governance and resilience.

Why This Matters Now

Under Australia's mandatory ransomware payment reporting regime, organisations with annual turnover above \$3 million and certain critical infrastructure entities must report ransom payments to the Australian Cyber Security Centre within 72 hours. The iNews reporting highlights a confronting reality:

At least 75 Australian organisations with turnover above \$3 million reported paying ransoms in the first eight months of the regime

A further 19 payments came from critical infrastructure entities, taking the total to at least 94 known payments

Between 7 and 13 larger organisations are reporting ransom payments every month, suggesting that paying has become business as usual

This is happening despite clear guidance from the Australian Signals Directorate advising organisations not to pay ransoms. There is no guarantee of data recovery or non-disclosure, and payment often increases the likelihood of further attacks.

The Uncomfortable Truth

Organisations are rarely paying because ransomware attackers are exceptionally sophisticated. They are paying because, when an incident occurs, downtime costs, regulatory exposure and reputational damage feel worse than the ransom itself. In many cases, the payment was avoidable. Ransom payments are often framed as pragmatic decisions. In reality, they are frequently the outcome of discovering that critical plans do not work under real-world pressure.

The Real Reason Organisations End Up Paying

In practice, organisations end up paying ransoms when they discover, under pressure, that they are not operationally prepared to respond. Across incidents, the same weaknesses appear repeatedly.

Backups exist, but cannot be restored

Backups are present, but they are outdated, incomplete, untested or encrypted alongside production systems. Without proven restore capability, disaster recovery plans fail at the moment they are needed most.

No clear incident response authority

Without a concise, rehearsed ransomware response playbook, decision making becomes slow and fear driven. Roles, escalation paths and authority are unclear, particularly after hours.

No practical business continuity plan

Without a current BCP, organisations do not understand how to operate critical services in a degraded state. Manual workarounds, service prioritisation and alternate processes have not been defined.

Communications are unrehearsed

Boards, customers, regulators, insurers and the media receive inconsistent or delayed messaging. This amplifies perceived damage and increases pressure to pay. In short, ransom payments are usually a symptom of weak IR, DR and BCP disciplines, not an unavoidable outcome of modern cyber threats.

What Good Looks Like Under RealWorld Pressure

Having policies documented is not the measure of readiness. The real test is whether they work at 2am on a long weekend.

Incident Response

Effective ransomware incident response includes:

A concise, ransomware-specific response playbook

Clear decision paths for isolation, shutdowns and escalation

Defined triggers for engaging legal counsel, public relations, cyber insurance and law enforcement

Unambiguous authority and accountability, including after hours

When an incident occurs, there should be no debate about who decides or what happens next.

Disaster Recovery

Disaster recovery is more than having backups. Strong DR capability includes:

Offline, immutable backups for critical systems

Clearly defined RPOs and RTOs aligned to business impact

Regular testing of full system restores, not just file recovery

Honest measurement of how long recovery actually takes

If full restores have not been tested, recovery capability is unknown.

Business Continuity Planning

A practical BCP focuses on keeping the business running through disruption:

Identification of truly critical processes

Defined manual workarounds and reduced service models
Clear understanding of dependencies across people, technology and suppliers
Validation that critical vendors can support you during an incident
Business continuity turns chaos into managed disruption.

Tabletop Exercises

Resilient organisations rehearse before it matters. Effective ransomware tabletop exercises:
Simulate realistic ransomware and extortion scenarios
Involve executives and operational leaders, not just IT
Test difficult decisions such as system shutdowns, customer notification, regulator engagement and data leak threats
Every exercise should conclude with clear remediation actions and ownership. The goal is not compliance. It is confidence.

Making Paying the Ransom the Worst Option

When Incident Response, Disaster Recovery and Business Continuity are aligned and tested, organisations regain control. Paying the ransom should feel like the least attractive option on the table. With mandatory reporting now in place, ransomware carries regulatory, legal, reputational and ethical consequences. Preparation is no longer optional. It is a governance obligation.

Final Thought

Ransomware is not just a technical problem. It is a test of leadership under pressure. Organisations that invest in tested incident response, disaster recovery and business continuity planning protect their customers, their reputation and their future. If your plans have not been tested recently, now is the time. A short discussion with Barry Sollitt, our vCISO, can help validate whether your current IR, DR and BCP arrangements would stand up under real-world pressure. Let's talk about when those plans should be tested next.

According to you, why does paying a ransomware ransom represent a failure of preparation?

We explain that organisations end up paying ransoms when they discover, under pressure, that they are not operationally prepared to respond. Ransom payments are usually a symptom of weak Incident Response (IR), Disaster Recovery (DR) and Business Continuity Planning (BCP) disciplines, not an unavoidable outcome of modern cyber threats.

What does Australia's mandatory ransomware payment reporting regime require?

Under Australia's mandatory ransomware payment reporting regime, organisations with annual turnover above \$3 million and certain critical infrastructure entities must report ransom payments to the Australian Cyber Security Centre within 72 hours.

What is the Australian Signals Directorate's guidance on paying ransoms?

The Australian Signals Directorate advises organisations not to pay ransoms, noting there is no guarantee of data recovery or non-disclosure, and that payment often increases the likelihood of further attacks.

What common weaknesses cause organisations to end up paying ransoms, ?

The article identifies four recurring weaknesses: backups that exist but cannot be restored (outdated, incomplete, untested, or encrypted alongside production systems); no clear incident response authority (unclear roles, escalation paths, and authority, especially after hours); no practical business continuity plan (no defined manual workarounds or service prioritisation); and unrehearsed communications (inconsistent or delayed messaging to boards, customers, regulators, insurers and media).

What makes for strong Disaster Recovery capability ?

Strong DR capability includes offline, immutable backups for critical systems; clearly defined RPOs and RTOs aligned to business impact; regular testing of full system restores (not just file recovery); and honest measurement of how long recovery actually takes.

What should a practical Business Continuity Plan (BCP) focus on?

A practical BCP focuses on identification of truly critical processes, defined manual workarounds and reduced service models, clear understanding of dependencies across people, technology and suppliers, and validation that critical vendors can support the organisation during an incident.