SHOULD YOU PAY THE RANSOM?

AN INSIDE LOOK AT WHY ORGANISATIONS PAY

CLOUDGUARD

Introduction: Why this question matters

As the old saying goes, ransomware attacks are not a matter of if, but when. And when your organisation is in the hot seat, the toughest question isn't how the attackers got in (though you'll need to answer that too).

It's this: Should we pay the ransom?

This guide walks you through a simulation based on a ransomware event that unfolded inside a UK manufacturing company, with £94M in revenue, 1,000+ customers and just one IT manager left in place.

They faced:

- No working backups
- Orders worth millions about to miss delivery
- A live ransom note sent to the CEO's personal LinkedIn inbox
- And a £500K demand with the clock ticking

In the end, they paid. **But it didn't solve the problem.**

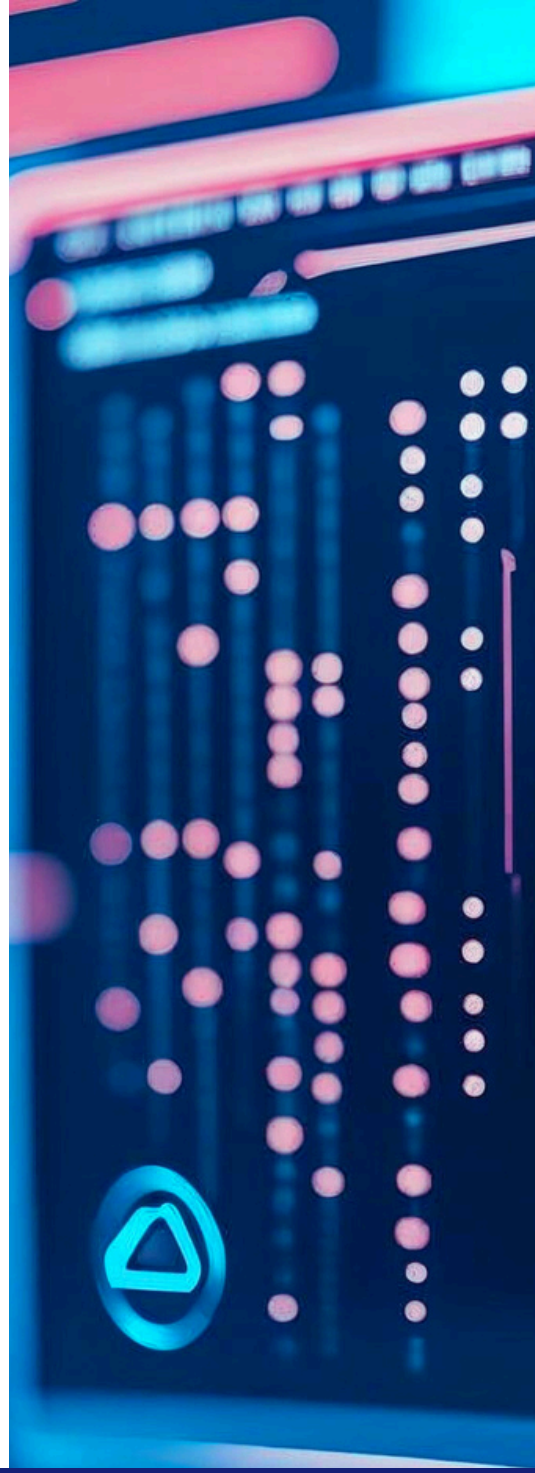
Inside, you'll see how the decision unfolded, as well as the cost models and the emotional strain. Most importantly, you'll learn what they **would do differently** and how your team can prepare before it's your turn in the war room.

Use this guide to understand:

- How ransomware attacks really unfold (it's faster than you think)
- What makes the decision to pay so complex, messy and high-stakes
- Why paying the ransom doesn't guarantee recovery or resolution
- The critical conversations your board, legal and IT teams must have before an attack hits

CloudGuard's legal position

- CloudGuard advises **very strongly against** paying a ransom
- Every company position is different
- This guidance is general in nature
- The content herein does NOT override specific laws and regulations that apply in the UK
- The **ultimate decision** whether to pay a ransom is with the victim
- Legal position - It is **illegal** to pay a ransom if you know or suspect the proceeds are going to a terrorist organisation
- Under the "payment prevention regime", a new legal duty to **disclose intent** to pay cyber criminals to restore access to systems and data is proposed



Organisations do pay ransoms

United Healthcare

£16.2M in March 2024
Paid Alphv/BlackCat

CDKGlobal™

£18.5 M in June 2024
Paid BlackSuit

cencora

£55M in March 2024
Paid Dark Angels

Snapshot: The company

Name: Personalised Widgets

Size: 120 employees

Sector: UK manufacturing, serving oil, gas, utilities and military contracts

IT Team: 3 staff (2 resigning, 1 working notice period)

Annual Revenue: £94M

Cyber Insurance: Basic coverage with some support for ransomware claims

Key metrics	2024 values
Revenue	£94M
Gross Profit	£28M
Net cash	£17.6M
Cyber insurance	£1M

The company had over 1,000 global customers and dealt with highly-customised valve manufacturing. Despite the firm's healthy £28M gross profit and £17.6M cash position, investment in cybersecurity had been repeatedly **deprioritised** in favour of operational output.

The three-person IT team was stretched thin, covering infrastructure, endpoint management, security and user support. Two staff had handed in notice weeks earlier, citing lack of progression and workload pressure. At the time of the attack, only **one IT manager** remained and was already working his notice period.

With major orders due to ship on Monday and regulatory compliance tied to multiple sectors, the business couldn't afford extended **downtime**.

Stage 1: The attack

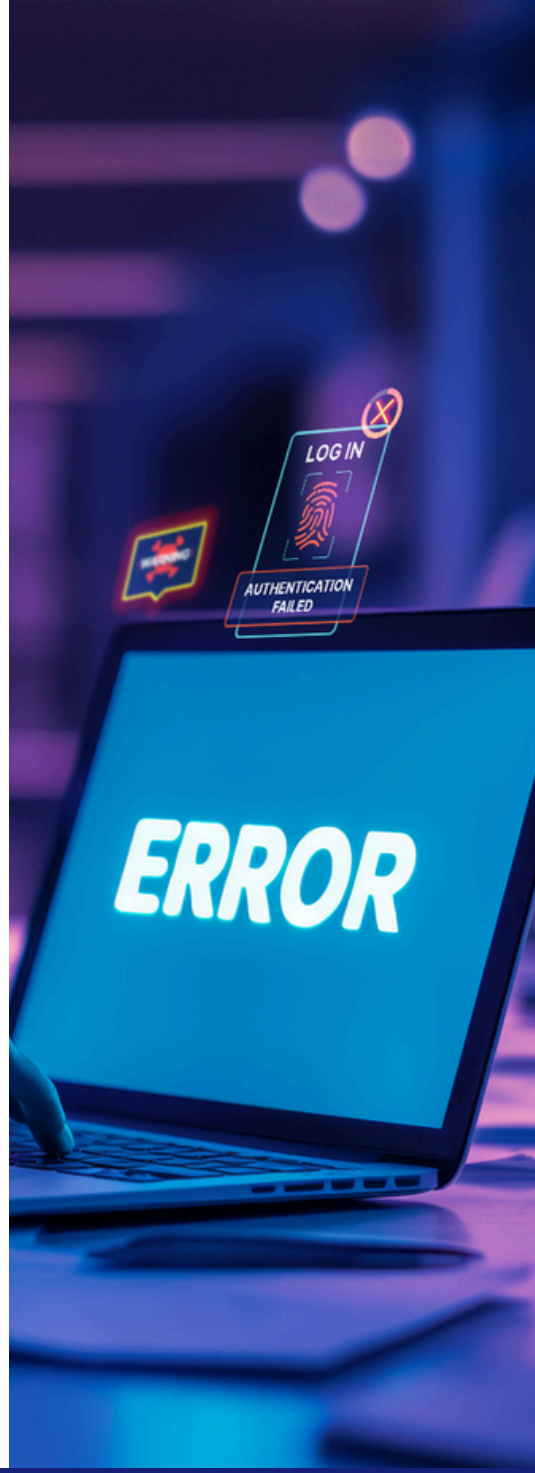
Friday PM: The Finance team processes a legitimate supplier payment. It is later determined that the supplier's request may have been leveraged for phishing or lateral movement.

- **Friday 3:00 PM:** Production ends for the week. IT identifies small corruption and attempts restoration.
- **Saturday:** Threat actors begin full lateral movement, privilege escalation and disable AV tools.
- **Sunday 6:47 AM:** CEO receives a ransomware message via LinkedIn. Full infrastructure is compromised.
- **Sunday 7:30 AM:** IT confirms ransomware encryption and likely data exfiltration. Board is notified.
- **8:30 AM:** Crisis meeting called.

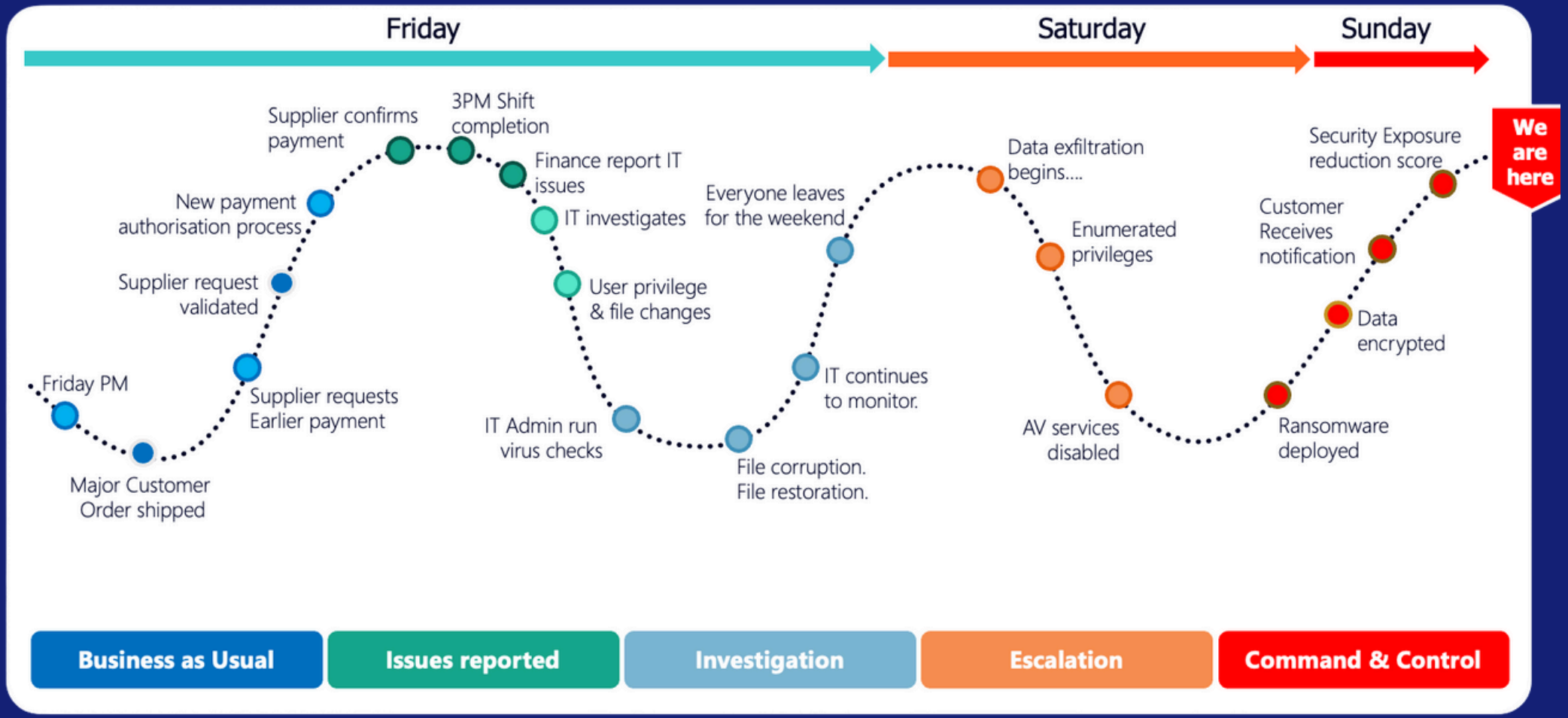
The attackers had already been in the system for weeks, utilising an MFA session token reuse and an unpatched SAP vulnerability. Logs showed outbound data transfer to a service called *Rising Sun*.

Issues were reported and highlighted.

The Board knew of the issues and proceeded at risk.



Stage 1: The attack



Stage 2: The business impact

The board met urgently at 8:30 AM Sunday. Here's what they were told:

- Production was fully down
- ERP, emails and files were all encrypted
- No recent or safe backups existed
- Rebuild time was estimated at 10 days
- Cost of downtime: £225,000/day
- Two critical orders were due to ship Monday morning

Known Risks:

- **Data theft and GDPR exposure** - especially if design files and customer contracts were exfiltrated
- **Supply chain breach notifications** - major clients would need to be informed, triggering scrutiny and potential liability
- **Penalties for delayed client orders** - will affect engagement and future orders
- **Long-term brand damage**- 45 years of customer relationships that had been built on reliability were now in jeopardy

That's your sneak peek

CLOUDGUARD

Security Done Different

Complete the form to access the full guide