

Crisis contained

Minimal loss, maximum control

Policy Triggered: Cyber



Proactivity

Chubb acted immediately, deploying a coordinated team of legal, forensic, and PR experts. By identifying payroll as the critical risk, the response focused on business continuity from the outset, not just breach containment.



Technical Ability

Vendors rapidly stood up a disaster recovery environment, enabling partial system restoration and manual processing. Forensics and IT specialists worked around the clock to stabilise operations despite severe encryption and data loss.



Solutions Focussed

Rather than defaulting to rigid processes, Chubb and its partners tailored a strategy that got payments out fast, kept contractors in place, and reassured clients, minimising reputational and financial fallout.

1. The Event

A Vice Society ransomware attack encrypted systems and leaked 71GB of sensitive data. Chubb was notified immediately and deployed panel legal, forensic, and PR teams to coordinate response, recovery, and regulatory compliance.

2. The Impact

The insured's operations ground to a halt – no email, no payroll, no applicant processing. Sensitive data on 40,000+ contractors and employees was exfiltrated, including ID documents and financial details.

3. The Problem

The attack hit days before payroll. With 85,000 contractors awaiting payment, business continuity and reputation was at risk. Missing payroll could lead to walkouts, lost placements, and long-term commercial damage.

4. The Solution

Chubb's vendors worked with the insured to quickly restore limited systems in a disaster recovery environment, enabling manual payments using prior records. Clear comms reassured contractors and clients, easing pressure on frontline teams.

5. The Outcome

Payroll went out on time, safeguarding operations and relationships. The business avoided reputational fallout, contractor loss, and customer churn with minimal complaints and no claims arising from the event.

