


 [info@archerround.au](mailto:info@archerround.au)

 1800 841 224

 <https://www.archerround.com>



ARCHER & ROUND

30 years of Cybersecurity Excellence



**Archer & Round Cybersecurity Report**

# Ransomware Trends and Resilience Strategies for 2025

**June 2025 Edition**



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

## 30 years of Cybersecurity Excellence

### Executive Summary

Ransomware remains the most damaging and costly cyber threat globally in 2025. Despite increased awareness, attacks have grown in sophistication, speed, and impact. Attackers are now leveraging double extortion, AI-driven intrusion tactics, and supply chain vulnerabilities to maximise damage. This report outlines the latest ransomware trends and provides resilience strategies that businesses can adopt to reduce their risk and accelerate recovery.

### Key Findings

#### **Ransomware Attack Volume Continues to Climb.**

Sophos reports a 27% global increase in ransomware attacks in 2024, driven by more aggressive threat actors and automated attack tools.

#### **Double Extortion is Now the Norm.**

Attackers no longer just encrypt files — they also steal data and threaten public release to force payment.

#### **Supply Chain Ransomware Attacks are Surging.**

Palo Alto Networks highlights a rise in attacks through vulnerable suppliers, software vendors, and third-party service providers.

#### **Critical Industries Are Top Targets.**

Healthcare, education, energy, and government sectors face relentless attacks due to their limited tolerance for downtime.

#### **Speed to Encryption Has Sharply Decreased.**

The ACSC warns that modern ransomware can encrypt entire systems in as little as 10 minutes after initial compromise.



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

## 30 years of Cybersecurity Excellence

### Key Ransomware Trends in 2025

TREND	DESCRIPTION	EXAMPLE
Double Extortion	Data theft plus encryption	Attackers leak stolen data if ransom unpaid
AI-Driven Attacks	Automated lateral movement and credential theft	AI used to find and exploit weaknesses faster
Supply Chain Compromise	Infiltrating software vendors and service providers	Kaseya-style ransomware via third-party software
Ransomware-as-a-Service (RaaS)	Toolkits and playbooks sold to less-skilled attackers	Fast, templated attacks by low-tier cybercriminals
Rapid Encryption	Faster payload deployment	File encryption completed in under 10 minutes

### Case Study: Supply Chain Ransomware Attack

In 2024, a global logistics provider was compromised via a third-party software update that was seeded with ransomware. The incident encrypted thousands of endpoints across 15 countries, halting shipping operations for five days and leading to millions in recovery costs and lost revenue.

**Source:** Palo Alto Networks 2024 Ransomware Report



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

## 30 years of Cybersecurity Excellence

### Resilience Strategies for 2025

Ransomware remains the most damaging and costly cyber threat globally in 2025. Despite increased awareness, attacks have grown in sophistication, speed, and impact. Attackers are now leveraging double extortion, AI-driven intrusion tactics, and supply chain vulnerabilities to maximise damage. This report outlines the latest ransomware trends and provides resilience strategies that businesses can adopt to reduce their risk and accelerate recovery.

#### 1. Build a Tested Backup and Recovery Process

Ensure you have offline, immutable backups that are regularly tested for fast recovery.

#### 2. Enforce Multi-Factor Authentication (MFA) Everywhere

Prevent credential-based access by applying MFA across all endpoints, cloud services, and critical systems.

#### 3. Segment Your Network

Use network segmentation to limit lateral movement and isolate high-value assets.

#### 4. Keep All Systems and Software Updated

Patch frequently and minimise the use of outdated or unsupported systems.

#### 5. Educate Employees on Phishing and Social Engineering

Run ongoing security awareness training to reduce the likelihood of successful phishing attempts.

#### 6. Monitor for Early Signs of Compromise

Deploy endpoint detection and response (EDR) tools and continuously monitor for suspicious activity.



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

## 30 years of Cybersecurity Excellence

### Global Best Practices and Guidelines

- Australian Cyber Security Centre (ACSC) Essential Eight
- NIST Cybersecurity Framework
- ENISA Ransomware Guidelines
- Cybersecurity and Infrastructure Security Agency (CISA) Ransomware Prevention Best Practices

### The Bottom Line: Prepare, Don't React

Ransomware will remain a significant threat in the coming years, but businesses that prioritise prevention, detection, and recovery planning will dramatically reduce their risk. A resilient organisation is one that can withstand an attack and recover swiftly, minimising both financial and reputational damage.

#### Recommended Resources:

- Australian Cyber Security Centre – Ransomware Guidance
- Sophos State of Ransomware 2024
- Palo Alto Networks Threat Intelligence

#### Archer & Round Cyber Intelligence Team

Safe | Secure | Reliable

Contact us: [info@archerround.com](mailto:info@archerround.com)