cowbell

Cyber Threats Targeting the Waste Management & Recycling Sector

Notable incidents, threat actors, and mitigations for waste services organizations

Executive Summary

The waste management and recycling sector is an often overlooked yet critical component of national infrastructure. In recent years, cybercriminals have shifted their focus to this sector, recognizing that waste services are highly vulnerable due to thin profit margins, limited cybersecurity budgets, and an increasing reliance on connected digital technology.

From commercial collection fleets to highly automated recycling facilities, the sector faces an escalating barrage of ransomware, Business Email Compromise (BEC), and supply chain attacks. Because waste management organizations cannot afford extended operational downtime without causing severe environmental and public health disruptions, threat actors hold significant leverage during extortion negotiations. This white paper outlines the current global threat landscape, profiles notable incidents across the US, UK, and Australia, and provides a sound approach to risk management and operational resilience.

Matthieu Chan Tsin
SVP & General Manager, Cowbell Resiliency Services

Strengthening cyber resilience alongside tailored cyber insurance is crucial to avoiding catastrophic losses. Cowbell Resiliency Services equips policyholders with the tools and expertise to proactively detect and mitigate vulnerabilities, fortify infrastructure, and counter evolving threats.

Additional questions? Request a consultation.

Our experts are happy to explain the process in more detail and address any issues you may have.

Notable Cyber Incidents: United States

Across the US, the waste management sector represents a unique risk configuration. These businesses are heavily tied to municipal contracts, where any service interruption triggers strict contractual penalties and a public relations crisis. Furthermore, as waste services digitize their logistics and routing platforms, a single ransomware incident can halt commercial collection fleets overnight - severely impacting cash flow. Policyholders must be helped to look beyond standard General Liability and Commercial Property coverages to ensure they have an adaptive cyber policy capable of funding specialized forensic response and business interruption recovery.

BFI Waste Services (US)

In a recent ransomware incident, a major regional division suffered an environment-wide network encryption event. The attack completely locked staff out of automated route optimization systems, forcing dispatchers to manage collection schedules manually with pen and paper. The disruption resulted in localized backup of commercial waste and substantial extra expenses to deploy temporary alternative logistics platforms.

Zero-Day Exploit on Fleet Management Software

Threat actors targeted a widely used third-party automated logistics provider in the US, gaining remote code execution privileges. The breach exposed the personal and financial data of thousands of corporate municipal clients.

Notable Cyber Incidents: United Kingdom

In the UK, waste management and recycling facilities are increasingly recognized as critical suppliers. An attack on these entities doesn't just disrupt a single business; it ripples through local councils and manufacturing supply chains. Downtime from a cyberattack can quickly lead to severe regulatory fines if waste processing violates environmental laws. We must ensure that UK waste service operators protect their Buildings & Contents and secure robust Cyber policies with rapid-response triage capability.

Claud Bilbao
VP, Underwriting & Distribution UK & Australia

Viridor Recycling (UK)

A sophisticated double-extortion ransomware attack targeted internal corporate networks, exfiltrating hundreds of gigabytes of sensitive administrative data, employee records, and municipal contract tenders. When the organization maintained its stance against paying the ransom, the threat actors published the stolen documents on a dark web leak site.

Biffa plc Systems Disruption

An opportunistic phishing campaign successfully harvested administrative credentials, allowing threat actors to compromise internal procurement portals. This led to a sophisticated business email compromise (BEC) scheme where vendor payment instructions were altered, resulting in the fraudulent diversion of significant operational funds before the breach was contained.

Notable Cyber Incidents: Australia

Australian waste and resource recovery operations are facing a strict new regulatory reality. Under recent privacy and critical infrastructure updates, the financial and reputational fallout of a data breach can be catastrophic for a mid-market operator. We have seen specialized waste processors targeted by syndicates who aggressively weaponize exfiltrated data to force compliance. The Australian market plays an indispensable role in helping these policyholders understand that security choices dictate operational survival, and that a standalone cyber policy is critical to safeguarding their future.

Anthony Wall
Head of Underwriting (Australia)

Cleanaway Waste Management

In a highly coordinated attack, a ransomware syndicate gained initial access via an unpatched public-facing application. The attackers moved laterally into systems managing automated sorting facilities and weighbridge data, threatening a complete operational shutdown if their financial demands were not met. Cleanaway successfully deployed its incident response plan to isolate the threat, though full remediation required weeks of forensic oversight.

JJ's Waste & Recycling (Social Engineering Campaign)

Attackers utilized a highly targeted vishing (voice phishing) campaign, impersonating technical support staff to gain remote access to endpoint devices. The incident compromised internal financial databases and customer account records.

Threat Actor Profiles

Ransomware operators targeting the waste services sector are primarily financially motivated, capitalizing on the sector's low tolerance for operational downtime.

- **LockBit & AlphV (BlackCat):** Prolific RaaS groups that regularly target critical infrastructure, utilizing double-extortion tactics to threaten the release of corporate tenders and client financial details.
- **Medusa:** Known for exploiting unpatched remote access tools, Medusa frequently leverages dark web countdown clocks to apply extra emotional pressure on mid-market organizations.

The Sound Approach to Risk: Recommendations

Digital risks are real, but they are manageable with sound protection. Waste management organizations should look to prioritize:

1. **Enforce Multi-Factor Authentication (MFA):** Implement phishing-resistant MFA across all remote access services, corporate email accounts, and fleet dispatch portals to neutralize credential harvesting.
2. **IT and OT Network Segmentation:** Isolate automated sorting machinery, weighbridge systems, and industrial processing controls from the general office internet and email networks to prevent ransomware from moving laterally.
3. **Establish Clear DFIR Playbooks:** Develop and regularly test Digital Forensics and Incident Response playbooks. Knowing exactly how to isolate a compromised server and who to call within the first hour minimizes downtime and preserves community trust.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0072 0626