covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

The Executive Guide to Backup & Recovery

How mid-size organisations can achieve verifiable resilience.

This guide is authored for the strategic leaders of mid-sized organisations who shoulder the weight of operational continuity. While the technical architecture of data protection remains a primary IT function, the ultimate responsibility for organisational resilience now resides firmly within the boardroom.

Whether you are an IT Director tasked with orchestrating recovery across fragmented hybrid environments, a CISO navigating the rigorous mandates of NIS2 and DORA, or a CEO evaluating the reputational risk of prolonged downtime, this document provides the clarity required to move from hope to verification.

Mid-market entities often find themselves in a unique position: managing enterprise-grade complexity without the benefit of enterprise-scale budgets. This guide is designed to bridge that gap. It offers a pragmatic blueprint for building a '**Recovery First'** culture - one that prioritises the rapid restoration of services over the mere storage of data.

By the end of this guide, senior leaders in IT and Operations should gain a clear understanding of what 'good' looks like right now, from the nuances of SaaS protection to the practical application of the 3-2-1-1-0 rule. It is an essential resource for those who recognise that in an era of industrialised cybercrime, the ability to recover is the ultimate competitive advantage.

Contents

Executive summary

Ransomware and cyber incidents are now business-as-usual risks rather than edge cases. Recovery is often measured in millions of pounds and weeks of disruption, with hidden costs in lost customers, reputation and staff time.

At the same time, regulators and insurers are treating operational resilience as a board-level obligation. Frameworks such as the EU's Digital Operational Resilience Act (DORA), NIS2 and the UK's Cyber Security and Resilience Bill - along with specific sector guidance and tightening cyber insurance standards - all ask a similar question:

- **Can you prove that you can recover quickly and safely when the worst happens?**

This guide sets out what 'good' looks like today. It explores why traditional backup alone no longer guarantees recovery in a world of Multi-Cloud, SaaS and AI-driven attacks. It explains how to design recovery led objectives (RPO and RTO) that reflect how your business actually runs, what is and is not covered in Microsoft 365 and other SaaS platforms and how to protect them properly, and how to bring on premises, Azure, AWS, Google Cloud and other workloads together into a single, orchestrated recovery model using a comprehensive multi-environment backup and recovery platform.

We also look at how modern security controls, including SOC and SIEM, phishing defences, penetration testing and cyber insurance, intersect with backup and recovery. Drawing on Covenco's real world experience with existing customers, we outline what to do in the first hours of a major incident and how to prove your approach works through regular rebuild and recovery testing backed by meaningful KPIs.

Covenco's Enterprise Data Protection & Recovery Framework underpins this guide. It combines the modern 3-2-1-1-0 rule with tiered recovery objectives, dependency-aware planning and a ring-fenced private cloud built specifically for backup and recovery at pace.

We close with a practical call to action: a complete **Backup & Recovery Gap Analysis** for your organisation, where Covenco specialists help you benchmark your current posture and define a roadmap to verifiable resilience.

Why Backup & Recovery matter now more than ever

Cyber incidents now hit mid-size organisations as often as global enterprises. Ransomware gangs increasingly use automation and AI-driven tooling to move from initial compromise to data exfiltration and encryption in minutes rather than days.

When incidents occur, the pattern is familiar. Downtime is measured in days or weeks, especially where domain controllers or cloud identity platforms are affected. Recovery costs covering forensics, rebuild, emergency consultancy and lost revenue, often exceed any ransom demand, even if no ransom is paid. Paying an attacker offers no guarantee of complete or reliable decryption and can invite repeat targeting.

Regulators and insurers have responded. DORA, for example, requires financial entities to maintain ICT business continuity, to test backup and recovery plans at least annually and to operate segregated backup systems with documented restoration procedures. Similar expectations appear through GDPR, sector specific codes of practice, Cyber Essentials Plus and increasingly detailed cyber insurance questionnaires.

For senior leaders the message is blunt. Having some backups is no longer enough. You must be able to show that you can recover quickly and safely, under pressure, from a worst-case scenario. Resilience is not about avoiding every incident. It is about being confident you can switch the lights back on quickly when they go out.

Where traditional Backup strategies break down

Most backup strategies have evolved organically. Each new application, cloud service or data centre has been 'added into backup' with whatever tools and time were available. The result is frequently a patchwork of technologies, schedules and responsibilities. When a serious incident hits, the cracks in that patchwork become painfully evident.

The 'we forgot the map' problem

In one Covenco engagement, a customer hit by ransomware had carefully backed up file servers, databases and virtual machines, but not the domain controller that told everything else where to go. When it was time to restore, nothing would come back cleanly. It was like having a box of puzzle pieces without the picture on the lid.

Only by finding an old physical server, an ex-domain controller leaning against a wall in a cupboard, were engineers able to extract a recent copy of the directory database and rebuild a new, secure domain controller. Without that stroke of luck, the business might have spent a year rebuilding identity and access, with serious risk to its survival.

The lesson is simple. Control planes such as directory services, identity platforms, configuration databases, orchestration tools and licensing servers are as critical as the data itself. If they are not explicitly included in backup and in recovery testing, you do not really have a plan.

Assuming 'the cloud has got it'

Moving workloads into Microsoft 365 or public cloud is often treated as handing resilience over to someone else. While providers offer highly resilient infrastructure, their shared responsibility models are clear: you are responsible for your data.

Gaps appear when organisations do the following:

- Rely on Microsoft 365 recycle bins and retention policies instead of a true backup outside Microsoft's domain.
- Fail to back up configuration, identity and networking alongside cloud data.
- Assume that multi zone or multi region deployments are equivalent to a tested DR plan.

When a misconfigured script, privilege escalation, or API error breaks your failover mid-incident, that assumption fails.

For senior leaders the message is blunt. Having some backups is no longer enough. You must be able to show that you can recover quickly and safely, under pressure, from a worst-case scenario.

Backup as a compliance checkbox

Traditional backup practice focused on retention, keeping copies for years at the lowest cost. Tapes in a vault satisfied audit questions but often took days or weeks to restore.

Even modern disk or cloud backup can let you down if no one has attempted a full restore in years, if runbooks exist only as forgotten documents, or if supposedly immutable snapshots can be altered or deleted via compromised management consoles. True cyber resilience depends on structured plans and repeatable testing, not simply on accumulating more copies of data.

Treating cyber incidents like traditional disasters

In a conventional disaster such as fire, flood or extended power loss, rapid failover is usually the right response. In a cyber incident that mindset can be dangerous. If a threat actor still has a foothold in your environment, bringing systems up as fast as possible may simply offer them a second chance to destroy or encrypt recovered systems.

Covenco distinguishes between two approaches:

- Conventional disaster recovery, which prioritises rapid failover and continuous replication.
- Cyber recovery, which prioritises containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced.

Runbooks you cannot reach

It remains common to find DR plans and recovery runbooks stored only on the very systems they are supposed to help recover. In some cases, password vaults and encryption keys live on those same servers.

A runbook you cannot reach creates false confidence in peacetime - and panic on the day.

At minimum, recovery plans must be accessible offline and off the main network, stored with trusted partners such as Covenco and your incident response provider, and practised often enough to become part of how the organisation operates.

Covenco's view of modern Data Protection & Resiliency

Covenco's Enterprise Data Protection & Recovery Framework was built in response to these realities. At its heart is a simple idea: Your Backup is all about the Recovery.

Covenco is not a cyber security vendor. Our focus is on backup and recovery for our customers. When an existing Covenco customer suffers a major incident, we work alongside their incident response and security partners to help them return to service in a controlled, defensible way.

Verifiable resilience, not blind faith

The framework aligns technology, process and people around three outcomes:

- Resilience: The ability to recover critical services within defined RPO and RTO targets, even when a primary data centre or cloud account has failed or been compromised.
- Audit-ready compliance: The ability to evidence appropriate backup, recovery and testing to regulators, auditors and insurers.
- Operational confidence: IT leaders can sleep at night because recovery has been rehearsed, not simply documented.

Resilience is about proving that you can recover. That proof comes from immutable backups, multiple copies, documented runbooks and DR tests that stand up under scrutiny.

The 3-2-1-1-0 rule

Covenco applies the 3-2-1-1-0 standard:

- 3 copies of your data (production, plus two backups).
- 2 different media or platforms.
- 1 copy off site.
- 1 immutable or air-gapped copy.
- 0 unrecoverable errors, demonstrated through regular restore testing and monitoring.

In most environments this translates to primary production storage, a local fast recovery copy on modern disk or immutable object storage, and a copy in Covenco's private cloud. That cloud copy is logically and physically separated from your own infrastructure and provides a clean, independent recovery option for Covenco customers. Tape-out remains useful where long term 'gold copy' retention is required by regulation or cost.

Covenco's independent recovery cloud

Covenco's cloud is not a general-purpose hosting platform. It is engineered specifically for backup, recovery and temporary high availability for customers with Covenco services in place.

It has a ring-fenced design separate from your own cloud accounts and data centres, so failures or compromises there cannot easily spread into backups. Storage, connectivity and orchestration are tuned for fast ingest and rapid large-scale recovery, rather than steady state production workloads.

In serious incidents, Covenco can run critical workloads in its cloud for a limited period while your primary environment is rebuilt, before failing you back in an orderly way. Where latency, regulation or local equipment demand it, we can also relocate Disaster Recovery infrastructure on site.

Core infrastructure patterns

From an infrastructure perspective, strong backup and recovery today looks like a layered pattern rather than a single appliance or SaaS product.

On premises estates typically involve modern virtualisation, such as VMware, Hyper-V or Nutanix, for core workloads - alongside remaining physical servers. Storage platforms, such as IBM FlashSystem with SVC, provide reliable hardware snapshots and replication that complement backup software with instant readiness. A central backup engine, frequently Veeam, protects virtual and physical workloads and delivers application aware backup for databases, directory services and messaging. Local immutable storage provides short term, high speed restores.

In the cloud, Azure, AWS and GCP workloads, including PaaS databases and object storage, require native or cloud aware backup. Network and identity design must support recovery into alternative regions or even different clouds, not just back to the original platform.

For SaaS, Microsoft 365 and other critical services need dedicated backup to a platform outside the provider's own tenancy. All of these layer's feed into Covenco's private cloud, which becomes the independent recovery anchor for customers using our services.

Understanding RPO and RTO

Recovery Point Objective (RPO) describes how much data you can afford to lose, measured as the time between the last good backup or snapshot and an incident. Recovery Time Objective (RTO) describes how quickly you need a system back in a usable state after an incident.

The instinctive demand for zero data loss and instant recovery across every system is understandable, but rarely affordable or necessary. A better approach is to classify workloads into tiers and make explicit trade-offs.

In cyber incidents especially, speed and safety must be balanced. Accepting a slightly slower recovery can be the right choice if it allows for a clean rebuild after forensic work, rather than recreating an environment that remains compromised.

Designing for Recovery: RPO, RTO and Dependency-Aware planning

A credible strategy begins with a shared view of what 'good recovery' looks like in your organisation. That means aligning backup with how the business actually operates, not only with the underlying infrastructure.

The vendor landscape and why Covenco leads with Veeam

The backup market is crowded. In practice, mid-size and enterprise organisations tend to focus on a small set of serious contenders. Covenco has chosen to make Veeam the backbone of much of our service portfolio because it delivers:

- Data locality and sovereignty, so backups can land in Covenco's cloud, on your hardware or in defined regions.
- Data freedom, so workloads backed up from VMware, Nutanix or Azure can be restored on alternative platforms.
- Recent improvements including hardened appliances, stronger immutability options, continuous data protection and deeper storage integration.

Other vendors such as Rubrik, Commvault - and SaaS first solutions like Druva or Keepit are valuable in the right scenarios. In every case, the recovery strategy comes first, and product selection follows.

An example tiering model

In most environments a simple four tier model works well:

Tier 0 **Foundational Control**	Active Directory or Entra ID, domain controllers, identity, DNS, core configuration repositories.
Tier 1 **Business Critical**	ERP, finance, HR, core line of business applications, key customer facing systems.
Tier 2 **Important**	Departmental applications, intranets, collaboration tools.
Tier 3 **Non-critical**	Test and development environments, historical archives.

Tier 0 has the tightest RPO and RTO, Tier 3 the loosest. Covenco's framework visualises this with Recovery Tier Objectives and clear sequencing, so Tier 0 comes back first, then Tier 1, and so on.

Mapping your dependencies

Real incidents rarely expose only the obvious systems. They reveal hidden dependencies, for example the HR platform that still relies on an old SQL server, the e-commerce site that needs a forgotten licensing server, or the cloud workload that refuses to start without particular firewall rules and DNS entries.

A practical dependency map for each key service should note:

- Which identity and directory services it relies on.
- Which databases and storage volumes underpin it.
- Which network segments, DNS zones and firewalls it depends on.
- Which external SaaS platforms or third-party APIs it calls.
- The first iteration does not need to be perfect, but it must be detailed enough to drive a realistic recovery sequence.

Covenco's consultants often begin with workshops, then convert the results into structured documentation and, where possible, scripts and automation.

Runbooks and decision making under stress

On the worst day, the weak point is rarely the technology. It is people and process.

A good runbook for major recovery has clear approval paths so it is understood who can authorise data loss beyond a certain RPO, who can approve aggressive containment actions, and who signs systems back into service. It defines a communication tree so IT, security, suppliers, executives and staff know who will brief them and how often, and there is no ambiguity about who speaks to insurers or regulators.

It includes a technical pre-flight checklist confirming clean administrative credentials are available, DR plans are accessible outside the affected infrastructure, and backup repositories are reachable and showing recent restore points. Recovery is sequenced by business priority, based on an agreed tiered list of applications and services. The idea of deciding what to do on the day is explicitly ruled out.

Finally, the runbook must remain current and accessible. It should be reviewed at least quarterly and after major changes and stored offline, with Covenco and with your incident response partner. A one-page summary checklist works well when pressure is high.

The Education Sector:
Protecting Microsoft 365 & SaaS

Microsoft 365 has become the standard platform for email and collaboration and, in education, for teaching and learning. Many schools, colleges and universities assume Microsoft is backing everything up, but the reality is more nuanced.

Legislative Drivers and Audit Readiness

Regulators and insurers are treating operational resilience as a board-level obligation. For the UK education sector, this means aligning with the UK GDPR and strict statutory standards for safeguarding data retention. Frameworks such as NIS2 and the UK's Cyber Security and Resilience Bill ask a similar question: can you prove that you can recover quickly and safely when the worst happens?

Educational institutions are increasingly subject to supply-chain and compliance audits from research partners, governing bodies, and cyber insurers. To remain compliant and secure funding, leadership must ensure verifiable data resilience that stands up to external scrutiny.

The Shared Responsibility Model

Microsoft guarantees the availability of the service, such as Exchange Online, SharePoint and Teams, but customers remain responsible for their own data. That includes protection against accidental deletion, malicious insiders and ransomware.

Built in features such as litigation hold, recycle bins and retention policies are valuable, but they are not full backup strategies. Backups should live outside Microsoft 365's own tenant and administrative domain, and organisations need to be able to restore at multiple granularities, from a single email or document to an entire mailbox, site, team or tenant.

Risks Particular to Education

Educational establishments have a distinctive risk profile:

- High user churn as students and staff join and leave.
- Highly sensitive safeguarding and pastoral records.
- Teaching materials spread across Teams, SharePoint class sites and OneDrive.
- Constrained IT budgets and small IT teams.

In that context it is easy for a departing member of staff to permanently delete vital teaching materials, or for ransomware to spread through synchronised OneDrive folders and encrypt both local and cloud copies. Misconfigured retention policies can remove leaver data that should have been kept for statutory periods. Shared mailboxes or Teams used for safeguarding or SEND support can disappear without a proper backup.

Educational organisations need to be able to restore at multiple granularities, from a single email or document to an entire mailbox, site, team or tenant.

➔ Solutions for The Education Sector

To guarantee compliance and audit-readiness, organisations can deploy robust solutions through a managed provider. For education, Covenco recommends:

- Frequent backups of Exchange Online, OneDrive, SharePoint, Teams and key Azure AD objects into Covenco's private cloud.
- Retention tuned to regulatory requirements for examinations and safeguarding.
- Restore options from individual items up to entire mailboxes, sites, teams or tenants.
- Immutable copies of backup data to guard against ransomware.
- Coverage, where technically feasible, for key third-party SaaS tools integrated with Microsoft 365.
- Clear ownership for Microsoft 365 data protection, usually with the Head of IT or Director of Digital Learning.

To deliver this, Covenco commonly uses Veeam Backup for Microsoft 365, tailoring its application specifically to the demands of the education sector. This ensures data lands in locations under joint control and can be seamlessly incorporated into wider disaster recovery tests.

By leveraging Veeam, institutions can protect dynamic collaborative environments like classroom Teams and shared safeguarding mailboxes, ensuring critical teaching materials and pastoral records are preserved against accidental deletion or malicious encryption.

For very large college or university tenants, Veeam's own Data Cloud or other SaaS options may make sense. However, to guarantee audit-ready resilience, we consistently recommend maintaining an independent copy held securely with Covenco wherever possible.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Education Sector Data Resilience: Strategic Benchmarks

The UK education sector represents one of the most significant surfaces for cyber-risk, with institutions safeguarding vast quantities of sensitive personal data alongside high-value intellectual property. As schools and universities lean further into hybrid learning and 'Smart Campus' technologies, the disruption caused by a breach extends far beyond financial loss, directly impacting student outcomes and safeguarding commitments.

91%

Number of Universities Experiencing Ransomware

Higher Education remains the most targeted sub-sector in the UK, with 91% of universities identifying at least one cyber breach or attack from 2025 to 2026.

Source: UK Gov: Cyber Security Breaches Survey 2025

£3m

Maximum Ransomware Impact per School Incident

While ransom demands vary, the total financial impact of a single ransomware event on a UK school - including recovery and emergency IT support - can reach up to £3 million.

Source: ESS SIMS: The Rising Cost of Cyber Attacks on UK Schools

50%

Improvement in Rapid Recovery Readiness

There is a positive trend in resilience; 50% of lower education providers were able to fully recover from a ransomware attack within a single week in 2025, up from 30% the previous year.

Sophos: State of Ransomware in Education 2025

£440,000

Daily Cost of Educational Downtime

For larger institutions and Multi-Academy Trusts (MATs), the estimated daily cost of downtime during a major system outage is approximately £440,000, factoring in lost productivity and emergency remediation.

Source: ESS SIMS: UK School Cyber Statistics 2025

92%

AI-Powered Phishing Concern

A significant majority (92%) of education IT leaders now rank AI-driven phishing as the most dangerous emerging threat for the 2025/26 academic year, surpassing even traditional ransomware.

Source: Cybersecurity in Education Report 2025–2026

2-9 months

Duration for Full System Restoration

While initial operations may resume sooner, the timeframe for a total, forensic-level restoration of all educational and administrative systems following a breach is typically between two and nine months.

Source: UK Gov / ESS SIMS: Impact of Cyber Attacks on Schools

The Energy Sector: The Primary Target for Industrial Control Systems Attacks

The Energy sector was the primary target for Industrial Control Systems attacks in 2025, accounting for 30% of global incidents, with critical SCADA vulnerabilities increasing by 25% year-on-year and ransomware attempts targeting backup infrastructure reported by one in four energy firms; the average cost of an energy data breach reached $5.12 million, while failure to comply with resilience standards could result in fines up to £17 million, and by 2026, 75% of energy organisations are expected to unify OT and IT security under a single CISO to address the dissolving air-gap.

25%

Increase in SCADA Vulnerabilities

Critical vulnerabilities in SCADA and industrial networks reached a record high in 2025, representing a 25% year-on-year increase in the exposure of operational technology.

Source: Claroty: State of XIoT Security Report 2025

$5.12m

Average Cost of an Energy Data Breach

The average cost of a data breach within the Energy sector has risen to $5.12 million, reflecting the extreme complexity and forensic requirements of recovering distributed and remote assets.

Source: IBM - Cost of a Data Breach Report 2025

1 in 4

Targeted Backup Infrastructure Frequency

Recent analysis shows that 1 in 4 energy firms reported a ransomware attempt specifically targeting their backup infrastructure to prevent grid or system restoration.

Source: Veeam - 2025 Ransomware Trends Report

£17m

Potential Non-Compliance Fines

Failure to meet resilience standards such as the NCSC Cyber Assessment Framework (CAF) or NIS2 can result in administrative fines of up to £17 million or 4% of annual turnover for essential service providers.

Source: NCSC UK: Cyber Assessment Framework (CAF) Guidance

The Energy Sector
Protecting Critical Infrastructure

For the energy sector, data loss and system downtime extend far beyond financial impact; they represent a direct threat to national infrastructure and public safety. As operations become increasingly digitised, the assumption that critical grids and supply networks are isolated from traditional IT threats is no longer valid.

Legislative Drivers and Audit Readiness

Regulators and insurers are treating operational resilience as a board-level obligation. For UK energy providers, regulatory scrutiny is intensifying through the strict requirements of the NCSC Cyber Assessment Framework (CAF), alongside frameworks such as NIS2 and the UK's Cyber Security and Resilience Bill. These regulations ask a similar question: can you prove that you can recover quickly and safely when the worst happens?

Energy companies must also navigate complex supply-chain audits. Partners, government bodies, and cyber insurers increasingly require verifiable proof of resilience. Treating backup as a compliance checkbox with tapes in a vault that take days to restore is no longer acceptable. Leadership must demonstrate structured, tested recovery plans that protect both corporate data and operational technology environments.

Risks Particular to Energy

The energy sector possesses a unique and highly targeted risk profile:

- IT and OT Convergence: The historical air-gap between Information Technology (IT) and Operational Technology (OT), such as SCADA systems, is dissolving, creating new pathways for attackers to reach critical control systems.
- Geographically Dispersed Assets: Infrastructure spans remote wind farms, offshore rigs, and unstaffed substations, complicating local recovery efforts.
- Aggressive Threat Actors: Ransomware gangs increasingly use automation and AI-driven tooling to move from initial compromise to data exfiltration and encryption in minutes rather than days.
- Legacy Systems: Critical infrastructure often relies on older, fragile systems that are difficult to patch and back up using standard modern tooling.

In this environment, bringing systems up as fast as possible following a cyber incident can be dangerous, potentially offering an attacker a second chance to destroy or encrypt recovered systems.

Leadership in the Energy Sector must demonstrate structured, tested recovery plans that protect both corporate data and operational technology environments.

➔ Solutions for the Energy Sector

To guarantee compliance and operational continuity, energy providers must move beyond basic backups to engineered cyber recovery. Through Covenco's managed services, organisations can implement solutions tailored for critical infrastructure:

- **Strict Application of the 3-2-1-1-0 Rule:** Ensuring three copies of your data, on two different media, with one copy off site, and critically for energy grids, one immutable or air-gapped copy - all with zero errors.
- **Clean Room Recovery:** Prioritising containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced to the production grid.
- **Dependency-Aware Planning:** Explicitly mapping and protecting Tier 0 foundational controls - such as Active Directory, identity, and core configuration repositories- so that the control planes controlling the OT environments come back online first.
- **Independent Recovery Cloud:** Utilising Covenco's independent recovery cloud, which has a ring-fenced design separate from your own cloud accounts and data centres, ensuring compromises cannot easily spread into backups.

By anchoring their recovery strategy with Covenco and technologies like Veeam, energy executives can ensure their environments are protected by hardened repositories, role-based access, and anomaly detection. This approach translates into audit-ready compliance and the operational confidence that power can be restored swiftly and securely under pressure.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

The Healthcare Sector
Protecting Patient Data & Clinical Systems

In healthcare, system disruption is not merely a financial or reputational issue; it is a direct risk to patient safety. As hospitals and private care providers digitise patient records and rely heavily on connected medical systems, robust data protection is paramount.

Legislative Drivers and Audit Readiness

Regulators and insurers are treating operational resilience as a board-level obligation. For UK healthcare providers, compliance is driven by the NHS Data Security and Protection Toolkit (DSPT), alongside frameworks such as NIS2 and the UK's Cyber Security and Resilience Bill. Specific sector guidance in Healthcare and Pharmaceuticals, along with tightening cyber insurance standards, all ask a similar question: can you prove that you can recover quickly and safely when the worst happens?

Furthermore, healthcare organisations must be prepared for rigorous supply-chain audits from partners, commissioning boards, and cyber insurers. Treating backup as a compliance checkbox is insufficient. To pass audits and secure funding, leadership must demonstrate verifiable resilience, not blind faith.

Risks Particular to Healthcare

The healthcare sector faces a highly challenging and specific risk profile:

- Targeted Cyber Threats: Ransomware gangs increasingly use automation and AI-driven tooling to move from initial compromise to data exfiltration and encryption in minutes rather than days. Highly sensitive patient data is incredibly lucrative on the black market.
- Zero Tolerance for Downtime: Clinical environments operate 24/7. When incidents land, downtime is measured in days or weeks, especially where domain controllers or cloud identity platforms are affected, which can severely impact patient care.
- Complex Infrastructure: A mix of legacy applications, modern Electronic Patient Record (EPR) systems, and connected medical devices creates a broad attack surface and hidden dependencies.
- Dangerous Recovery Assumptions: In a cyber incident, bringing systems up as fast as possible may simply offer threat actors a second chance to destroy or encrypt recovered systems.

To pass audits and secure funding, leadership must demonstrate verifiable resilience, not blind faith.

Solutions for the Healthcare Sector

To guarantee compliance and operational continuity, healthcare IT leadership must implement structured, dependency-aware recovery plans. Through a managed provider like Covenco, trusts and private providers can achieve the following:

- **Tiered Recovery Objectives:**
  Implementing an example tiering model, ensuring Tier 0 foundational controls such as Active Directory, identity, and DNS are recovered first, followed by Tier 1 business critical systems like core line of business applications and clinical records.
- **The 3-2-1-1-0 Standard:**
  Maintaining three copies of your data, on two different media, with one copy off site, and critically for energy grids, one immutable or air-gapped copy - all with zero errors.
- **Clean Room Recovery:**
  Prioritising cyber recovery over rapid failover, using containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced.
- **Independent Recovery Cloud:**
  Storing critical backups in Covenco's independent recovery cloud, which has a ring-fenced design separate from your own cloud accounts and data centres, ensuring compromises cannot easily spread into backups.

Behind the scenes, Covenco frequently leads with Veeam to protect virtual and physical workloads and deliver application aware backup for critical clinical databases and directory services. By leveraging Veeam's integration with SIEM and SOC platforms, Anomaly Detection, and Hardened Repositories, Covenco can help healthcare executives ensure they are audit-ready and capable of restoring life-saving services safely and securely under pressure.

Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Healthcare Data Resilience: Strategic Benchmarks

As Integrated Care Systems (ICS) increasingly use remote monitoring and AI-driven triage, the measure of success has shifted from total prevention to 'unbreakable' resilience - the ability to maintain clinical operations whilst under active adversarial pressure.

$7.42m

Average Cost of a Healthcare Data Breach

While the global average cost of healthcare breaches has fallen, the sector remains the costliest industry for the 14th consecutive year, with a single incident averaging $7.42 million.

Source: IBM - Cost of a Data Breach Report 2025

58%

Resilience Improvement: Recovery within One Week

Healthcare organisations have made significant progress in recovery readiness; 58% of providers were able to recover from a ransomware attack within a week in 2025, more than double the 21% reported in 2024.

Source: Sophos - State of Ransomware in Healthcare 2025

21%

Surge in Healthcare Cyber Incidents

The volume of cyber incidents affecting the healthcare sector climbed by 21% year-on-year in 2025, part of a broader 55% surge in incidents across all critical infrastructure sectors.

Source: Health-ISAC - Health Sector Heartbeat 2025

3x

Triple Threat: Rise in Extortion-Only Attacks

The rate of data theft without encryption - where attackers exfiltrate patient records for extortion- has tripled since 2023, making it the fastest-growing threat vector in healthcare.

Source: Sophos - State of Ransomware in Healthcare 2025

241 days

Median Breach Lifecycle

Globally, the time to identify and contain a data breach fell to a 9-year low of 241 days in 2025, though this still leaves a significant window for lateral movement and data theft.

Source: IBM - Cost of a Data Breach Report 2025

100%

Mandatory NHS DSPT Compliance

All organisations processing NHS patient information must provide annual assurances via the Data Security and Protection Toolkit (DSPT) to ensure safety and secure funding.

Source: NHS Digital Care Hub - DSPT Guidance 2025-26

Pharmaceutical Cyber Resilience: Protecting Intellectual Property & Production

The Pharmaceutical sector is now officially classified as critical infrastructure. With the tightening of the NIS2 Directive and the introduction of the Cyber Resilience Act (CRA), pharmaceutical boards face direct liability for the security of their global supply chains and the integrity of Manufacturing Execution Systems (MES).

$4.61m

Average Cost of a Pharmaceutical Data Breach

The cost of a data breach in the pharmaceutical sector reached an average of $4.61 million in 2025, driven by the high value of research data and the regulatory complexity of breach notification.

Source: IBM - Cost of a Data Breach Report 2025

191

Ransomware Attacks on Pharma & MedTech

In one year, 191 ransomware attacks specifically targeted businesses operating within the broader healthcare supply chain, including pharmaceutical and medical manufacturers.

Source: Comparitech - Healthcare Ransomware Roundup 2025

87%

Third-Party Ecosystem Breach Impact

The vast majority (87%) of pharmaceutical and healthcare organisations reported being negatively affected by a cybersecurity breach within their third-party ecosystem, underlining the risk of complex global supply chains.

Source: Help Net Security - Pharma Cybersecurity Risks 2025

€15m

Cyber Resilience Act Penalties

Non-compliance with the new Cyber Resilience Act (CRA) carries severe financial risks for pharmaceutical firms, with potential penalties reaching €15 million or 2.5% of global annual turnover.

Source: TTMS - Cyber Resilience Act in Pharma 2026

24 hours

Mandatory Incident Reporting Window

From September 2026, pharmaceutical organisations will be obligated to report security incidents within just 24 hours under new UK and EU legislative standards, necessitating highly orchestrated response plans.

Source: TTMS - Cyber Resilience Act in Pharma 2026

40%

Intellectual Property Theft in AI Breaches

Breaches involving unauthorised 'Shadow AI' tools have a significantly higher impact on pharmaceutical firms, with 40% of such incidents resulting in the direct theft of sensitive intellectual property.

Source: IBM - Cost of a Data Breach Report 2025

The Pharmaceutical Sector
Securing Intellectual Property & Operational Continuity

The pharmaceutical industry represents a uniquely high-value target for threat actors. Compromised research and development (R&D) data, disrupted clinical trials, or halted production lines carry catastrophic financial, regulatory, and reputational consequences. For IT leaders in this space, safeguarding intellectual property and ensuring continuous manufacturing processes requires a highly sophisticated approach to data protection.

Navigating Legislative Scrutiny and Supply Chain Audits

Senior executives are facing mounting pressure to demonstrate absolute confidence in their recovery capabilities, as regulators and insurers now treat operational resilience as a board-level obligation. The UK's Cyber Security and Resilience Bill, NIS2, and distinct sector guidance for Pharmaceuticals all demand verifiable proof that an organisation can recover safely and swiftly following a worst-case scenario.

Furthermore, resilience is no longer viewed in isolation. Third party and supply chain risk is treated as part of the organisation's own resilience, meaning pharmaceutical firms face stringent audits from research partners, global distributors, and cyber insurers. In fact, mature backup and recovery are becoming prerequisites for insurance rather than the benefit of the policy.

Distinct Cyber Risks in Pharmaceuticals

The threat landscape for pharmaceutical manufacturing and research is severe:

- **Accelerated Exfiltration:**
  Ransomware gangs increasingly use automation and AI-driven tooling to move from initial compromise to data exfiltration and encryption in minutes rather than days. This 'double extortion' tactic is particularly devastating when highly sensitive R&D or trial data is involved.
- **The Danger of Rushed Recovery:**
  Treating a cyber attack like a traditional disaster, such as a power loss, can be highly dangerous. If threat actors maintain a foothold within laboratory or manufacturing networks, bringing systems up as fast as possible may simply offer them a second chance to destroy or encrypt recovered systems.
- **Complex Dependencies:**
  Pharmaceutical operations rely on a web of legacy laboratory equipment, modern ERP systems, and cloud-based analytics, meaning real incidents frequently reveal hidden dependencies that complicate the restoration sequence.

Engineering Audit-Ready Resilience with Covenco

To satisfy regulators and protect invaluable intellectual property, pharmaceutical IT leaders must implement highly structured, defensible recovery mechanisms. Partnering with a specialist managed solutions provider such as Covenco allows organisations to implement the Enterprise Data Protection & Recovery Framework.

Compromised research and development (R&D) data, disrupted clinical trials, or halted production lines carry catastrophic financial, regulatory, and reputational consequences.

➔ Solutions for the Pharma Sector

For the pharmaceutical sector, Covenco recommends several strategic deployments:

- **Cyber Recovery Clean Rooms:**
  Rather than immediate failover, Covenco prioritises containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced to production environments. This ensures malware is not pushed back into critical manufacturing or research networks.
- **Dependency-Aware Tiering:**
  Classifying systems into clear tiers is essential for a controlled response. Foundational Tier 0 components (such as Active Directory and identity platforms) must be restored first, enabling the secure recovery of Tier 1 business-critical applications like laboratory information management systems (LIMS).
- **Immutable Anchors:**
  Applying the 3-2-1-1-0 standard ensures there is always at least 1 immutable or air-gapped copy of critical data, shielded from administrative compromise.
- **Isolated Cloud Infrastructure:**
  Backups converge into a ring-fenced design in Covenco's independent recovery cloud, which is physically and logically separated from the primary data centres or cloud accounts where an attack occurred.

By placing Veeam at the core of this strategy, pharmaceutical organisations benefit from hardened repositories, anomaly detection, and tight integration with SIEM and SOC platforms.

This orchestrated approach elevates backup from a technical afterthought into a verifiable security asset, giving leadership the metrics and evidence required to satisfy the most demanding supply-chain and regulatory audits.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Food Processing & Production Sector
Safeguarding Supply Chains & Manufacturing Yields

Food production relies on highly synchronised, time-sensitive supply chains. A cyber incident in this sector does not just mean lost data; it means immediate physical consequences, from spoiled inventory and halted production lines to empty supermarket shelves.

Legislative Reality and Supply Chain Pressure

While the UK's Cyber Security and Resilience Bill updates the landscape domestically, UK food processors face intense international regulatory pressure. Frameworks such as the EU's Digital Operational Resilience Act (DORA), NIS2 and the UK's Cyber Security and Resilience Bill - along with tightening cyber insurance standards all ask a similar question: can you prove that you can recover quickly and safely when the worst happens?

For UK food manufacturers supplying European markets, demonstrating NIS2-aligned cyber resilience is rapidly becoming a prerequisite to passing stringent supply-chain audits from EU partners. At the same time, regulators and insurers are treating operational resilience as a board-level obligation.

For senior leaders the message is blunt: **Having some backups is no longer enough.**

Risks Particular to Food Production

The operational realities of food processing create distinct vulnerabilities:

- **IT and OT Convergence:**
  Production lines, temperature control systems, and automated logistics are increasingly connected to corporate IT, expanding the attack surface.
- **Latency and Legacy:**
  Facilities often rely on older Operational Technology (OT) and require systems to operate with near-zero latency, complicating modern backup agent deployment.
- **Rapid Spoilage:**
  When incidents land, the pattern is familiar. Downtime is measured in days or weeks, especially where domain controllers or cloud identity platforms are affected. For perishable goods, an extended outage guarantees catastrophic product loss.
- **Supply Chain Interdependence:**
  Real incidents rarely expose only the obvious systems. They reveal hidden dependencies, complicating recovery if logistics schedules or third-party distributor APIs are knocked offline.

Achieving Verifiable Resilience with Covenco

To protect manufacturing yields and maintain distributor confidence, food processors must move beyond the days where tapes in a vault satisfied audit questions but often took days or weeks to restore. Through Covenco's managed services, organisations can bring on premises, Azure, AWS, Google Cloud and other workloads together into a single, orchestrated recovery model using a comprehensive multi-environment backup and recovery platform.

Solutions for the Food Sector

For the food sector, Covenco recommends:

- **Relocatable DR Services:**
  Covenco provides disaster recovery contracts and relocatable services. This offers pre agreed access to Covenco engineers, facilities and hardware for customers under contract, allowing recovery into Covenco's data centres, into hyperscalers or onto relocatable equipment on your site, which is valuable in manufacturing and other latency sensitive environments.
- **The 3-2-1-1-0 Standard:**
  Covenco applies the 3-2-1-1-0 standard. This ensures three copies of your data (production, plus two backups), on two different media or platforms, with one copy off site, and critically, one immutable or air-gapped copy - all with zero errors.
- **Dependency-Aware Planning:**
  Explicitly mapping which databases and storage volumes underpin automated production lines to ensure they are recovered in the correct sequence.
- **Independent Recovery Cloud:**
  Those backups converge into a ring-fenced environment in Covenco's cloud with at least one immutable or air-gapped copy per workload family. It has a ring-fenced design separate from your own cloud accounts and data centres, so failures or compromises there cannot easily spread into backups.

By leading with Veeam, Covenco ensures data freedom, so workloads backed up from VMware, Nutanix or Azure can be restored on alternative platforms. This delivers audit-ready compliance: the ability to evidence appropriate backup, recovery and testing to regulators, auditors and insurers.

Ultimately, you must be able to show that you can recover quickly and safely, under pressure, from a worst-case scenario.

Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Safeguarding National Supply Chain Stability for the Food Production Sector

Data resilience is the primary safeguard for manufacturing yields and national supply chain stability. Operating in a high-volume, low-margin environment defined by 'Just-in-Time' delivery, even minor disruptions to Manufacturing Execution Systems (MES) or ERP platforms can lead to catastrophic waste and the loss of critical distribution slots. As the industry integrates further with IoT and smart factory technologies, the convergence of IT and OT has created a significant new attack surface.

£3.48m

Average Cost of an Industrial/ Manufacturing Data Breach

The average cost of a data breach in the industrial and manufacturing sector, including food production, rose to £3.48 million in 2025, primarily driven by the extreme costs of unplanned operational downtime.

Source: IBM - Cost of a Data Breach Report 2025

10%

Rise of Extortion-Only Attacks

Extortion-only attacks- where data is stolen but not encrypted to avoid early detection- now account for 10% of manufacturing incidents, specifically targeting recipe IP and distribution schedules.

Source: Sophos - State of Ransomware in Manufacturing 2025

1 in 10

Ransom Payments exceeding $5m

Amongst manufacturers who chose to pay a ransom in 2025, one in ten were forced to pay $5 million or more to restore time-sensitive production lines.

Source: Sophos - State of Ransomware in Manufacturing 2025

Ensuring Operational Continuity and Supply Chain Integrity in the Manufacturing Sector

Operational resilience is no longer an abstract goal but a critical requirement for maintaining production yields and supply chain integrity. The convergence of Information Technology (IT) and Operational Technology (OT) has significantly widened the attack surface, exposing legacy control systems to modern cyber threats. With the implementation of the NIS2 Directive and the NCSC's Cyber Assessment Framework (CAF), manufacturing must move from a posture of simple protection to one of engineered, verifiable recovery.

65%

Manufacturing Ransomware Incident Frequency

In 2025, 65% of manufacturing organisations reported being hit by ransomware, as attackers increasingly exploit the time-sensitivity of production lines for extortion.

Source: Sophos - The State of Ransomware in Manufacturing 2025

1 in 3

Supply Chain Entry Point Frequency

One in three cyber attacks on the UK manufacturing sector now originates via a third-party supplier or logistics partner, illustrating the inherent risks of integrated supply networks.

Source: Verizon - Data Breach Investigations Report 2025

53%

System Intrusion Dominance

System Intrusion remains the primary attack pattern in production environments, involved in 53% of all successful breaches affecting manufacturing infrastructure.

Source: Verizon - Data Breach Investigations Report 2025

The Manufacturing Sector
Sustaining Production & Supply Chain Integrity

For the modern manufacturing sector, data is as critical to the production line as raw materials. From complex Enterprise Resource Planning (ERP) software to automated shop floors, a cyber incident that halts IT systems inevitably stops physical output.

The Compliance and Audit Landscape

Manufacturers are deeply embedded in global supply chains, making them subject to rigorous external scrutiny. Frameworks such as NIS2 and the UK's Cyber Security and Resilience Bill directly impact the sector. Crucially, regulators and insurers are now treating operational resilience as a board-level obligation.

When tendering for major contracts or renewing cyber insurance, senior leaders are increasingly asked a similar question: can you prove that you can recover quickly and safely when the worst happens? Demonstrating audit-ready compliance - the ability to evidence appropriate backup, recovery and testing - is now a commercial necessity to retain key clients and partners.

Manufacturing-Specific Vulnerabilities

The operational realities of modern manufacturing introduce distinct risks:

- **Latency Sensitivity:**
  Many factory floor operations cannot tolerate the latency of cloud-based infrastructure and require localised computing power.
- **Complex Interdependencies:**
  Real incidents frequently reveal hidden dependencies, such as a core production platform that relies on an old SQL server or a forgotten licensing server.
- **IT and OT Convergence:**
  As operational technology (OT) becomes more connected to the corporate IT network, the attack surface broadens, allowing threat actors to move laterally from an office environment directly to the production line.
- **The Cost of Downtime:**
  Recovery is often measured in millions of pounds and weeks of disruption, with hidden costs in lost customers, reputation and staff time.

Demonstrating audit-ready compliance - the ability to evidence appropriate backup, recovery and testing - is now a commercial necessity to retain key clients and partners.

➔ Solutions for the Manufacturing Sector

To protect manufacturing yields and satisfy demanding supply-chain audits, IT leadership must implement robust, dependency-aware recovery mechanisms.

Through Covenco's managed services, organisations can build a strategy tailored to industrial environments:

- **Relocatable DR Services:**
  Recognising that cloud recovery is not always viable for shop floors, Covenco provides disaster recovery contracts with pre agreed access to engineers, facilities and hardware. This allows for recovery onto relocatable equipment on your site, which is exceptionally valuable in manufacturing and other latency sensitive environments.
- **Dependency-Aware Planning:**
  Covenco consultants execute structured documentation and dependency mapping to ensure foundational Tier 0 control planes (like Active Directory) are restored before Tier 1 business critical ERP systems.
- **Data Freedom and Agility:**
  By leading with Veeam, Covenco ensures data freedom, meaning workloads backed up from systems like VMware or Nutanix can be restored on alternative platforms if primary hardware is compromised.
- **The 3-2-1-1-0 Rule:**
  Applying this strict standard ensures there are three copies of your data, on two different media, with one copy off site, and critically for energy grids, one immutable or air-gapped copy - all with zero errors.

This engineered approach ensures that even if primary security controls are bypassed, manufacturers have a tested, documented path to rebuild their operations and satisfy the strictest auditor requirements.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

The Banking Sector
Ensuring Financial Stability & Compliance

For the banking sector, operational downtime and data breaches pose systemic risks to the wider economy. Consumer trust and market stability rely entirely on the continuous availability of critical banking services, making robust, verifiable recovery capabilities an absolute necessity.

Legislative Drivers and Audit Readiness

Regulators and insurers are treating operational resilience as a board-level obligation. The legislative landscape for banking is particularly rigorous, with frameworks such as the EU's Digital Operational Resilience Act (DORA), NIS2 and the UK's Cyber Security and Resilience Bill – along with specific sector guidance in financial services – all asking a similar question: can you prove that you can recover quickly and safely when the worst happens?

Regulators and insurers have responded. DORA, for example, requires financial entities to maintain ICT business continuity, to test backup and recovery plans at least annually and to operate segregated backup systems with documented restoration procedures. To satisfy these requirements and pass stringent audits from regulatory bodies like the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), institutions must achieve audit-ready compliance: the ability to evidence appropriate backup, recovery and testing to regulators, auditors and insurers.

Risks Particular to Banking

Banks face an exceptionally hostile threat landscape combined with highly complex internal IT environments:

- Ransomware gangs increasingly use automation and AI-driven tooling to move from initial compromise to data exfiltration and encryption in minutes rather than days.
- Recovery is often measured in millions of pounds and weeks of disruption, with hidden costs in lost customers, reputation and staff time.
- Most mid-size organisations now operate genuine hybrid estates. On premises servers, VMware or Hyper-V clusters and legacy applications sit alongside workloads in Azure and AWS, pockets of Google or IBM Cloud, and numerous SaaS platforms.
- If a threat actor still has a foothold in your environment, bringing systems up as fast as possible may simply offer them a second chance to destroy or encrypt recovered systems.

Institutions must achieve audit-ready compliance: the ability to evidence appropriate backup, recovery and testing to regulators, auditors and insurers.

➔ Solutions for the Banking Sector

To protect transactional integrity and satisfy DORA requirements, banking IT leadership must move away from treating backup as a compliance checkbox. Through Covenco's managed services, banks can implement an enterprise-grade recovery strategy:

- **Segregated Recovery Environments:** Covenco's cloud is not a general-purpose hosting platform. It has a ring-fenced design separate from your own cloud accounts and data centres, so failures or compromises there cannot easily spread into backups.
- **Structured Cyber Recovery:** Covenco distinguishes between conventional disaster recovery, which prioritises rapid failover, and cyber recovery, which prioritises containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced.
- **The 3-2-1-1-0 Rule:** Covenco applies the 3-2-1-1-0 standard. This guarantees three copies of your data, on two different media, with one copy off site, and critically for energy grids, one immutable or air-gapped copy - all with zero errors..
- **Dependency-Aware Tiering:** A simple four tier model works well, starting with Tier 0: foundational control Active Directory or Entra ID, domain controllers, identity, DNS, core configuration repositories.

To execute this, Covenco frequently leads with Veeam. Veeam includes security-oriented features, including integration with SIEM and SOC platforms, anomaly detection and hardened repositories backed by role-based access and multi factor authentication. This allows banking executives to sleep at night because recovery has been rehearsed, not simply documented.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Maintaining Transactional Trust and Digital Stability in the Banking Sector

The UK banking sector operates under the most stringent regulatory scrutiny in history, with the Digital Operational Resilience Act (DORA) and the Bank of England's resilience frameworks setting a high bar for digital stability. In an 'always-on' transactional environment, even minutes of downtime can lead to significant reputational damage and systemic risk. Executives must now ensure that recovery capabilities are not just present, but are orchestrated to meet granular Recovery Time Objectives (RTO) for core banking functions.

6.71 hours

Average Ransomware Response Time

UK financial institutions achieve an average ransomware response time of 6.71 hours, demonstrating the high-speed orchestration required to contain modern, automated threats.

Source: CyberSecStats - UK Cybersecurity Statistics 2026

99%

Payment-Related Incident Prevalence

Nearly all (99%) UK banking and finance leaders have experienced a payments-related cyber incident within the past 24 months, reflecting the persistent nature of digital fraud.

Source: CyberSecStats - UK Cybersecurity Statistics 2026

44%

Primary Regulatory Challenge

For 44% of financial institutions, the single most pressing operational challenge is maintaining compliance with evolving cyber security regulations, including DORA and NIS2.

Source: CyberSecStats - UK Cybersecurity Statistics 2026

2.4m

VIP-Targeted Phishing Volume

In the first half of 2025, 2.4 million phishing emails were observed targeting the financial sector, with 30% specifically aimed at high-value or executive users.

Source: Darktrace - The State of Cybersecurity in the Finance Sector 2026

214,000

Monthly DLP Incident Alerts

Data Loss Prevention (DLP) remains a persistent risk, with over 214,000 unauthorised data transfer attempts observed across the financial sector in a single month during late 2025.

Source: Darktrace - The State of Cybersecurity in the Finance Sector 2026

Navigating Regulatory Compliance and Data Sovereignty for Financial Services

For broader financial services firms- including wealth management, fintech, and investment houses - cyber resilience is the foundation of client trust and data sovereignty. As these organisations increasingly transition core workloads to the cloud, the complexity of managing distributed data risks has grown exponentially. Compliance with DORA is now a mandatory board-level obligation, requiring a shift from passive backup to active, verifiable recovery testing.

£5.74m

Average Cost of a UK Financial Services Breach

Financial services remains the costliest UK industry for data breaches, with the average incident cost reaching £5.74 million in 2025, an increase from previous years.

Source: IBM - Cost of a Data Breach Report 2025

55%

DORA Compliance Readiness Gap

Over half (55%) of global financial institutions report that they are not yet fully prepared to meet the mandatory requirements of the Digital Operational Resilience Act (DORA) by the 2026 enforcement deadlines.

Source: Hexnode - DORA in 2026 Strategy Guide

2% turnover

Regulatory Financial Exposure

Non-compliance with DORA's risk management and reporting standards carries severe financial risks, with potential penalties reaching 2% of total annual worldwide turnover.

Source: Hexnode - DORA in 2026 Strategy Guide

93%

Double Extortion Payout Failure

Amongst financial victims who pay a ransom, 93% still suffer from subsequent data theft and 'double extortion', proving that payment does not guarantee data security.

Source: CrowdStrike / Cobalt - Cybersecurity Roundup 2026

12.5%

Growth in Cybersecurity Investment

To address the AI-amplified threat landscape, global cybersecurity spending is forecast to increase by 12.5% in 2026, reaching a total of $240 billion.

Source: Gartner - Information Security Forecast 2026

Financial Services Sector
Securing Wealth Management, FinTech & Capital Markets

The broader financial services sector- spanning asset management, payment providers and FinTech - relies implicitly on data integrity and the continuous availability of digital platforms. A disruption to these services not only damages immediate revenue but profoundly undermines investor and market confidence.

Regulatory Pressures and Audit Preparedness

The regulatory environment governing UK financial services is undergoing a dramatic shift towards proactive resilience. Regulators and insurers are treating operational resilience as a board-level obligation. Frameworks such as the EU's Digital Operational Resilience Act (DORA), NIS2 and the UK's Cyber Security and Resilience Bill - along with specific sector guidance in financial services... and tightening cyber insurance standards all ask a similar question: can you prove that you can recover quickly and safely when the worst happens?

Regulators and insurers have responded. DORA, for example, requires financial entities to maintain ICT business continuity, to test backup and recovery plans at least annually and to operate segregated backup systems with documented restoration procedures.

Furthermore, DORA may apply most directly to major financial services firms, but its emphasis on defined objectives, segregated backups and regular testing provides a useful benchmark for almost any organisation. To meet these demands, senior executives must ensure they possess audit-ready compliance: the ability to evidence appropriate backup, recovery and testing to regulators, auditors and insurers.

Distinct Risks for Financial Services Providers

Firms operating within the financial services ecosystem face a unique combination of cyber threats and architectural challenges:

- **Aggressive Threat Actors:**
  Ransomware and cyber incidents are now business as usual risks rather than edge cases. Attackers target this sector specifically for financial gain and access to highly sensitive market data.
- **Complex Multi-Cloud Estates:**
  Moving workloads into Microsoft 365 or public cloud is often treated as handing resilience over to someone else. However, while these providers offer highly resilient infrastructure, their shared responsibility models are clear: you are responsible for your data.
- **Third-Party SaaS Reliance:**
  Many modern financial services rely heavily on external SaaS platforms or third-party APIs. Critical gaps appear when organisations rely on Microsoft 365 recycle bins and retention policies instead of a true backup outside Microsoft's domain.
- **The Cost of Disruption:**
  Recovery is often measured in millions of pounds and weeks of disruption, with hidden costs in lost customers, reputation and staff time.

➔ Solutions for Financial Services

To protect client assets and satisfy stringent regulatory audits, financial services leaders must transition from legacy backup methods to orchestrated cyber recovery. Through Covenco, firms can bring on premises, Azure, AWS, Google Cloud and other workloads together into a single, orchestrated recovery model using a comprehensive multi-environment backup and recovery platform.

- **Unified Multi-Cloud Protection:**
  A typical Covenco design protects workloads wherever they run, centralises backups into Covenco's private cloud and enables flexible recovery.
- **Dedicated SaaS Backup:**
  For SaaS, Microsoft 365 and other critical services a dedicated backup to a platform outside the provider's own tenancy is needed.
- **Independent Recovery Anchor:**
  Covenco's private cloud becomes the independent recovery anchor for customers using our services. It has a ring-fenced design separate from your own cloud accounts and data centres, so failures or compromises there cannot easily spread into backups.
- **Dependency-Aware Planning:**
  Covenco establishes clear sequencing, so Tier 0 comes back first, then Tier 1, and so on, ensuring that identity platforms and configuration databases are restored before critical trading or payment applications.

Behind the scenes, Covenco has made Veeam the backbone of much of our service portfolio. Veeam delivers data locality and sovereignty, so backups can land in Covenco's cloud, on your hardware or in defined regions, which is vital for compliance with UK and EU data residency laws. This strategic deployment delivers operational confidence because recovery has been rehearsed, not simply documented.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Insurance & Underwriting Sector
Protecting Risk Data & Meeting Carrier Standards:

For the insurance and underwriting sector, operational disruption impacts both the firm's balance sheet and the broader market's ability to manage risk. Holding vast repositories of sensitive claims, financial, and actuarial data makes these organisations prime targets for extortion, demanding a highly sophisticated approach to data protection.

Legislative Drivers and Audit Readiness

Regulators and insurers are treating operational resilience as a board-level obligation. Frameworks such as the EU's Digital Operational Resilience Act (DORA), NIS2 and the UK's Cyber Security and Resilience Bill – along with tightening cyber insurance standards all ask a similar question: can you prove that you can recover quickly and safely when the worst happens?

In a unique position, insurers themselves must adhere to the very standards they mandate for their policyholders. Insurers increasingly require evidence of off-site immutable backups, regular DR tests and runbook reviews, and integration with recognised security controls such as EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Management). Consequently, mature backup and recovery are becoming prerequisites for insurance rather than the benefit of the policy. To pass supply-chain and regulatory audits, leaders must evidence highly structured, tested recovery plans.

Risks Particular to Insurance and Underwriting

The operational realities of underwriting and claims processing expose firms to specific threats:

- Ransomware and cyber incidents are now business as usual risks rather than edge cases.
- Recovery is often measured in millions of pounds and weeks of disruption, with hidden costs in lost customers, reputation and staff time.

Firms often assume financial cover is enough, but cyber insurance can pay for incident response, forensics, business interruption and legal or notification costs, but it cannot transform an untested, fragile backup estate into a robust one. In a cyber incident that mindset can be dangerous. If a threat actor still has a foothold in your environment, bringing systems up as fast as possible may simply offer them a second chance to destroy or encrypt recovered systems.

Mature backup and recovery are becoming prerequisites for insurance rather than the benefit of the policy. To pass supply-chain and regulatory audits, leaders must evidence highly structured, tested recovery plans.

➔ Solutions for the Insurance Sector

Cyber insurance should be treated as a financial safety net built on top of sound engineering. Through a managed solutions provider like Covenco, insurance firms can implement an enterprise-grade framework to ensure audit-readiness.

Covenco distinguishes between conventional disaster recovery, which prioritises rapid failover and continuous replication, and cyber recovery, which prioritises containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced. To deliver this, Covenco's approach includes:

- **The 3-2-1-1-0 Standard:** Covenco applies the 3-2-1-1-0 standard. This methodology guarantees 3 copies of your data (production, plus two backups), 2 different media or platforms, 1 copy off site, 1 immutable or air-gapped copy, and 0 unrecoverable errors, demonstrated through regular restore testing and monitoring.
- **Segregated Cloud Infrastructure:** Backups converge into Covenco's independent recovery cloud. It has a ring-fenced design separate from your own cloud accounts and data centres, so failures or compromises there cannot easily spread into backups.
- **Advanced Security Integration:** To protect core workloads, Veeam includes security-oriented features, including integration with SIEM and SOC platforms, anomaly detection and hardened repositories backed by role-based access and multi factor authentication.

By deploying these engineered solutions, Covenco is helping underwriting leaders guarantee they are fully compliant and capable of proving their resilience to regulatory bodies and peer institutions.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Shifting Liability & Mandatory Control Standards for Insurance & Underwriting

The insurance and underwriting sector is experiencing a period of significant volatility as cyber risk and business interruption become the dominant global threats. For underwriters, the ability to assess an organisation's 'verifiable resilience' has become the primary metric for policy eligibility and pricing. As ransomware attacks continue to industrialise, the focus has shifted from simple perimeter security to mandatory controls, including immutable backups and multi-factor authentication.

54%

Increase in Ransomware Claims Frequency

Publicly disclosed ransomware cases increased by 54% in the first half of 2025, significantly impacting loss ratios across the cyber insurance market.

Source: QBE Insurance Group - Ransomware Report 2026

40%

Projected Ransomware Growth

Ransomware attacks are on track to increase by 40% by the end of 2026 compared to 2024, as threat actors leverage automated and AI-driven exploitation tools.

Source: QBE Insurance Group - Ransomware Report 2026

$275bn

Annual Global Ransomware Costs

By 2031, global annual ransomware damage costs are forecast to reach $275 billion, highlighting the long-term systemic risk to the global underwriting industry.

Source: Cybersecurity Ventures - Ransomware Forecast 2026

89%

Cyber Risk Planning Adoption

Nearly nine in ten (89%) organisations now have a formal plan to address cyber risk, reflecting the widespread recognition of cyber insurance and resilience as core business requirements.

Source: Aon - Global Risk Management Survey 2025

13%

Business Loss from Cyber Threats

Cyber risk and business interruption remain the top global threats, with 13% of businesses suffering direct financial loss from cyber incidents in the 2024-2025 period.

Source: Aon - Global Risk Management Survey 2025

Protecting Client Confidentiality & Reputation in the Service Industry

For the professional and client-led service industry, data is the primary asset and client confidentiality is the foundation of market reputation. These organisations are increasingly targeted not only for their own data, but as gateways into the supply chains of their larger clients. As hybrid working becomes a permanent fixture, the risk of data exfiltration and credential theft has intensified.

49%

Phishing Incident Rate

Nearly half of all businesses in the service sector have been targeted by phishing attacks over the past year, making it the leading initial access vector for credential theft.

Source: Kaseya - Cybersecurity Roundup 2026

57%

Unauthorised AI Data Usage

Over 57% of employees are now using personal GenAI accounts for work, with one-third admitting to uploading sensitive corporate data into unsanctioned tools.

Source: Gartner - Security Forecast 2026

12%

Credential and API Key Leakage Rate

Cases of leaked developer secrets, including hard-coded credentials and API keys, increased by 12% in 2025, exposing service firms to lateral movement and data theft.

Source: ReversingLabs - Software Supply Chain State of Play 2025

$244bn

Projected Global Security Spending

Global information security spending is projected to reach $244 billion in 2026, as organisations across the service industry invest heavily in cloud and identity security.

Source: Gartner - Information Security Worldwide Forecast 2026

2x

Software Supply Chain Attack Volume

Supply chain attacks targeting commercial software providers doubled in early 2025, highlighting the risk to professional services that rely on integrated third-party platforms.

Source: Cyble - Threat Intelligence Report 2026

The Service Industry Sector
Securing Client Trust & Supply Chain Integrity

For professional services, consulting, legal, logistics, and business process outsourcing (BPO) firms, client data and uninterrupted availability are the lifeblood of the operation. A cyber incident in the service sector immediately compromises client confidentiality, disrupts the delivery of critical business functions, and breaches commercial service level agreements.

Legislative Drivers and Supply Chain Audits

Regulators and insurers are treating operational resilience as a board-level obligation. While service businesses themselves might not always be the primary targets of specific financial or critical infrastructure regulations, they are entirely captured by the supply chain requirements of their regulated clients.

Frameworks such as the EU's Digital Operational Resilience Act (DORA), NIS2 and the UK's Cyber Security and Resilience Bill, along with specific sector guidance - and tightening cyber insurance standards - all ask a similar question: Can you prove that you can recover quickly and safely when the worst happens?

Crucially, third party and supply chain risk is treated as part of the organisation's own resilience, not something that can simply be passed on. This means service providers are subject to rigorous, flow-down compliance audits from their enterprise customers.

To retain contracts, bid for new tenders, and satisfy these external audits, leadership must demonstrate audit-ready compliance: the ability to evidence appropriate backup, recovery and testing to regulators, auditors and insurers.

Risks Particular to the Service Industry

Service providers face unique operational vulnerabilities:

- **High Cloud and SaaS Adoption:**
  Moving workloads into Microsoft 365 or public cloud is often treated as handing resilience over to someone else. While providers offer highly resilient infrastructure, their shared responsibility models are clear: you are responsible for your data.
- **Targeted Supply Chain Attacks:**
  Ransomware and cyber incidents are now business as usual risks rather than edge cases. Attackers frequently target service providers to leapfrog into the networks of their larger, more heavily defended regulated clients.
- **The Commercial Impact of Downtime:**
  Recovery is often measured in millions of pounds and weeks of disruption, with hidden costs in lost customers, reputation and staff time.
- **Unreachable Plans:**
  It remains common to find DR plans and recovery runbooks stored only on the very systems they are supposed to help recover. A runbook you cannot reach creates false confidence in peacetime and panic on the day.

➔ Solutions for the Service Industry

To pass stringent supply-chain audits and protect client data, service industry IT leaders must move from organic, fragmented backup processes to a structured framework. Covenco's Enterprise Data Protection & Recovery Framework underpins this guide.

Through Covenco's managed services, firms can secure their operations and guarantee compliance:

- **The 3-2-1-1-0 Rule:**
  Covenco applies the 3-2-1-1-0 standard. This guarantees 3 copies of your data (production, plus two backups), 2 different media or platforms, 1 copy off site, and 1 immutable or air-gapped copy - all with zero errors.
- **Independent Recovery Cloud:**
  Backups are directed to Covenco's independent recovery cloud. It has a ring-fenced design separate from your own cloud accounts and data centres, so failures or compromises there cannot easily spread into backups.
- **Microsoft 365 and SaaS Protection:**
  For SaaS, Microsoft 365 and other critical services need dedicated backup to a platform outside the provider's own tenancy.
- **Cyber Recovery Clean Rooms:**
  Covenco distinguishes between conventional disaster recovery, which prioritises rapid failover and continuous replication, and cyber recovery, which prioritises containment, forensics and clean room rebuild with security specialists validating data before it is reintroduced.

Covenco has chosen to make Veeam the backbone of much of our service portfolio. This structured approach elevates data protection from an IT function to a demonstrable business asset, providing a practical balance between speed and assurance, which is increasingly what regulators, insurers and boards expect.

➔ Next Steps

Talk to us about your resiliency challenges

Call: +44 (0)1753 732 000
Email: enquiries@covenco.com
Web: covenco.com

Bringing it all back together
Multi-Cloud & Hybrid Recovery

Most mid-size organisations now operate genuine hybrid estates. On premises servers, VMware or Hyper-V clusters and legacy applications sit alongside workloads in Azure and AWS, pockets of Google or IBM Cloud, and numerous SaaS platforms. Data is spread across multiple environments. From a recovery perspective, the key is not to anchor your backups to the same platform you are trying to protect.

A reference architecture

A typical Covenco design protects workloads wherever they run, centralises backups into Covenco's private cloud and enables flexible recovery.

On premises virtual machines and physical servers are protected by agent based or agent-less backup. Cloud workloads in Azure, AWS and GCP are backed up with cloud native tooling, including PaaS databases and object storage. SaaS platforms such as Microsoft 365 are protected via specialist backup engines.

Those backups converge into a ring-fenced environment in Covenco's cloud with at least one immutable or air-gapped copy per workload family. From there, services can be restored back to their original platform or elsewhere. Azure workloads can be recovered into Covenco's cloud or another region, and on premises workloads can be rebuilt in the cloud when that makes sense.

Using Veeam's data freedom capabilities, Covenco can move backups between hypervisors and clouds, reducing vendor lock in and supporting cloud to cloud migrations.

Beware hidden cloud lock-in

Lifting and shifting virtual machines into AWS or Azure is relatively complex to reverse. The more you use cloud native services and APIs, such as queues, functions and proprietary databases, the more dependencies you accumulate that are hard to recreate elsewhere.

This is not a reason to avoid cloud. It is a reason to understand and manage the lock in. Keeping data copies outside the primary cloud platform, distinguishing between services that are convenient and those that are critical to rebuild, and testing whether a reduced function version of a service could run on alternative infrastructure all help reduce risk.

Orchestration and documentation

Backing up is often the easier part. Orchestrating recovery across platforms is where complexity arises.

For key services we recommend scripting the provision of landing zones, including networks, subnets, routing and identity roles, so they can be created consistently in DR or cyber recovery scenarios. Data and configuration restore steps are automated or at least templated. Cutover plans describe when and how users will be moved to the recovered environment and, later, back again. Runbooks remain visual and straightforward so that operations staff can follow them under pressure.

In more mature environments, these steps are treated as code and version controlled, making changes visible and auditable.

Security, Compliance & Cyber Insurance

Backup and recovery used to be seen as the responsibility of infrastructure teams alone. Today, they sit firmly within the cyber security and compliance agenda.

Backup as an arm of cyber security

Modern attacks tend to follow a pattern: initial access, lateral movement and privilege escalation, attempts to cripple production systems, attempts to corrupt or destroy backups and exfiltration of data for double extortion.

SOC and SIEM tooling help detect and contain these stages but do not remove the need for resilient backups. Security controls reduce the likelihood and scope of compromise. Covenco's backup and recovery capability gives customers a path to rebuild even when controls are bypassed, provided those services were in place before the incident.

Veeam includes security-oriented features, including integration with SIEM and SOC platforms, anomaly detection and hardened repositories backed by role-based access and multi factor authentication. These capabilities work best when designed jointly with your security provider so alerts, investigations and recovery actions are coordinated.

Regulatory expectations

Across sectors, regulatory frameworks share common themes. Organisations are expected to understand where their data lives, including cloud regions and third-party processors. They must maintain appropriate, segregated backups for critical data and services and test backup and recovery regularly, with documented evidence. Third party and supply chain risk is treated as part of the organisation's own resilience, not something that can simply be passed on.

DORA may apply most directly to major financial services firms, but its emphasis on defined objectives, segregated backups and regular testing provides a useful benchmark for almost any organisation. At the same time personal accountability is increasing, so backup and resilience are no longer viewed as just an IT responsibility.

Crisis management
What to do when the worst happens

When a major incident hits, the first hours matter enormously. Covenco has supported existing customers through serious UK cyber incidents, including high profile cases where core services were disrupted. Those experiences have shaped a pragmatic playbook.

While recovery is most seamless and cost-effective for established contract holders, Covenco remains fully equipped to assist any mid-sized or enterprise-scale organisation during a disaster. A core advantage of our service is the ability to ship fresh hardware directly to a customer's site - usually pre-loaded with recovery data - ensuring organisations can restore operations swiftly even if existing hardware has been quarantined.

Things we wish every customer had already done

Experience suggests a handful of preparatory steps make a disproportionate difference. Customers are far better placed if they have backed up the backup server configuration off site so Veeam can be rebuilt quickly, enabled immutability on premises as well as in Covenco's cloud, run at least one full DR test with Covenco so people and processes are familiar, enabled Veeam security features such as multi factor authentication, dedicated service accounts and role based access with anomaly alerts, and documented clear RPO, RTO and recovery priorities shared beyond the IT team.

Cyber insurance: a safety net, not a solution

Cyber insurance can pay for incident response, forensics, business interruption and legal or notification costs, but it cannot transform an untested, fragile backup estate into a robust one. Insurers increasingly require evidence of off-site immutable backups, regular DR tests and runbook reviews, and integration with recognised security controls such as EDR and SIEM.

Mature backup and recovery are becoming prerequisites for insurance rather than the benefit of the policy. Cyber insurance should be treated as a financial safety net built on top of sound engineering, not as an alternative to doing the hard work.

Clean data and the Recovery Clean Room

Recovering quickly is only half the battle. You must also be confident you are not simply reintroducing malware.

For customers with Covenco backup services, we usually work alongside a specialist incident response provider to stand up a clean recovery environment in Covenco's cloud or another agreed location. Selected backups are restored into that environment and scanned with at least one additional malware engine to those used day to day. Only once recovered workloads behave as expected and pass scanning are they reconnected to production networks and opened to users. This approach provides a practical balance between speed and assurance, which is increasingly what regulators, insurers and boards expect.

➔ The first five moves during a crisis

1 Contain the blast radius
Work with your incident response partner and network team to isolate affected segments. In some cases that means physically disconnecting systems. In others it means applying targeted firewall and routing changes. These decisions carry commercial consequences and must be owned at the right level.

2 Preserve evidence
Avoid rebooting servers or deleting files simply to 'tidy up'. In regulated environments you may need to demonstrate who accessed what and when, and what left the organisation.

3 Validate backup integrity
Establish which backups exist, where they are, whether they are immutable and when the last known good restore points occurred. Covenco's Covenco One portal, built on Veeam Service Provider Console and Veeam ONE, provides a consolidated view of backup health, job status, restore points and configuration.

4 Confirm the scope of compromise
The SOC and incident response team identify affected systems and determine whether backup repositories or Veeam infrastructure have been targeted. This informs which restore points can be trusted.

5 Agree a recovery sequence
Once you know what you can recover from and what you must rebuild to, agree an order aligned with your recovery tiers.

Changing direction halfway through a major restore is technically possible but operationally painful. A single, agreed plan with all stakeholders represented is far better.

Proving it works
Testing, KPIs & Continuous Improvement

A backup you have never tried to restore is a liability waiting to be exposed. Regulators, auditors and cyber insurers now expect evidence of regular testing of ICT response, backup and recovery plans. The same evidence should matter to you.

Recovery exercises and rebuild testing

Covenco recommends several layers of testing:

- **Tabletop exercises** bring IT, security and business stakeholders together to walk through realistic scenarios, clarifying who decides what, how communication will work and which trade-offs the organisation is willing to accept.
- **Workload level restores tests** focus on individual servers, databases or Microsoft 365 items restored into non-production environments on a regular schedule. These confirm that point in time recovery is genuinely available.
- **Tier 0 and Tier 1 rebuild drills** go further, rebuilding foundational services and one or two critical applications into a sandbox or into Covenco's cloud. Real users, such as finance or operations staff, log in and verify they can perform key tasks.
- **A full DR rehearsal at least once a year** should test the entire plan from invocation and technical recovery through to validation by business users. A test that reveals no issues is not always a success - because often it means the scenario was not demanding enough.

Automated verification

Manual tests are essential but do not scale on their own. Covenco uses tools such as Veeam SureBackup and virtual labs, together with additional clean room scanners, to automate parts of verification. Virtual machines can be booted directly from backups in isolated environments, application-level checks confirm services are running, and recovered workloads can be scanned with extra malware tools.

These processes generate reports and dashboards showing which backups have been tested, how often and with what result. They can be tied to SLAs so restore testing becomes routine rather than a special project.

KPIs that actually mean something

To keep senior stakeholders engaged, metrics must have clear meaning. Covenco's framework focuses on three main KPIs.

1. **Backup success rates**
   The proportion of backup jobs completed successfully in the last 30 or 90 days. The target should be high, and failures should be investigated rather than accepted as normal.
2. **RTO adherence**
   How often recovery tests meet or beat the agreed recovery time objective. This connects technical performance directly to business expectations.
3. **Resilience score or checklist completion**
   Progress against a structured list of resilience controls.
   Typical items include:

   - Classification of critical workloads into tiers with defined RPO and RTO.
   - Explicit inclusion of domain controllers and identity platforms in backup scope.
   - Independent backup of Microsoft 365 and other SaaS.
   - At least one immutable or air-gapped copy for each workload family.
   - Encryption of backups in transit and at rest.
   - Documentation and off system storage of recovery runbooks.
   - Recent tabletop and restore exercises, including Tier 0 and Tier 1 rebuild tests.
   - Monitoring and alerts for backup failures and RPO breaches.
   - Regular review of backup scope as systems change.
   - Visible ownership and metrics at executive level.

Organisations that track these areas see their technical posture improve and gain a shared language for conversations between IT, security and business leaders.

What ‘Good’ looks like today

A mid-size organisation with a strong posture will typically have documented, tiered RPO and RTO objectives linked to business impact, signed off by business owners as well as IT. It will protect on premises, cloud and SaaS workloads under a single coherent framework, with an independent recovery cloud such as Covenco’s acting as the anchor.

It will apply the 3-2-1-1-0 rule in practice, with at least one immutable or air-gapped copy and clear plans for how that copy would be used. It will run regular recovery and rebuild tests at different levels, with evidence for regulators, auditors, insurers and the board. Backup and recovery will be integrated into the wider cyber security programme alongside SOC and SIEM, endpoint protection and user awareness.

Cyber insurance will be treated as an extension of sound engineering, not as a substitute for it. A small set of meaningful KPIs will track progress, and backup and recovery will be understood as an ongoing programme rather than a one-off project.

Above all, ‘good’ is not about buying the most expensive technology. It is about designing the right layers of backup and recovery for the risks you actually face and rehearsing them until you can rely on them on your worst day.

Clean ingestion and platform isolation

Verifiable resilience depends as much on the integrity of the backup copy as on its existence. Customer data arriving into Covenco’s cloud via Veeam Cloud Connect is inspected inline before it is committed to long-term storage, with Veeam’s malware detection engine scanning incoming restore points for indicators of compromise, suspicious file renames and abnormal data entropy that typically signal ransomware activity - flagging anomalies for review rather than silently accepting them, and often giving early warning before the customer’s own monitoring has raised an alert.

Equally, the platform itself is architected so that no single customer incident can propagate further. Each customer’s repository is logically segregated with dedicated credentials, isolated network paths and immutability enforced at the storage layer, controls that cannot be overridden from the customer’s administrative domain even with full domain admin credentials.

Management of the underlying platform sits entirely within Covenco’s own administrative boundary, protected by multi-factor authentication and role-based access. The practical effect is straightforward: a ransomware actor who has fully compromised a customer’s production estate cannot reach across into Covenco’s cloud to encrypt, delete or alter the off-site immutable copy, nor pivot from one tenant to another. This is what we mean by a ring-fenced recovery anchor.

How Covenco can help

Covenco exists to do one thing well: backup and recovery at pace. We do not sell generic cloud hosting or try to be all things to all people. We focus on helping our customers achieve verifiable resilience.

In a market crowded with low touch backup targets and price only calculators, Covenco’s approach is different. We start with discovery, taking time to understand your infrastructure, your data, your business priorities and your regulatory context. We design backup and recovery with your environment in mind, so performance technology is not being asked to operate in conditions it was never built for.

We then build in layers: on premises where that makes sense, in the cloud where appropriate and on tape where cost and legislation demand it, always with our independent cloud as a secure anchor point.

Day to day, we operate services through our Managed Services team using the Covenco One portal to monitor, report and act. We test with you, from routine restores to formal DR days and full-scale rehearsals. For existing Covenco customers, we stand alongside your security partners and insurers when incidents occur.

A Covenco engagement typically includes:

- **Backup resilience workshop:**
  With IT, security and business stakeholders to map workloads, RPO, RTO and dependencies against Covenco’s framework, identify gaps and align expectations between IT, CISO, CFO and other leaders.
- **Architecture and design:**
  Multi-Cloud and hybrid backup architectures that apply the 3-2-1-1-0 rule across on premises, cloud and SaaS, commonly using Veeam as the core data protection engine and combining modern immutable storage on premises and in Covenco’s cloud with optional tape for long term, low cost retention.
- **Managed backup and DR services:**
  Operating backup tooling, monitoring, testing and reporting, backed by Covenco’s private cloud. This includes proactive alerting on failures and SLA breaches, regular restore tests and recovery days, and guidance on runbook creation, ownership and review.
- **Disaster recovery contracts and relocatable services:**
  Pre-agreed access to Covenco engineers, facilities and hardware for customers under contract, allowing recovery into Covenco’s data centres, into hyperscalers or onto relocatable equipment on your site, which is valuable in manufacturing and other latency sensitive environments.

Complimentary Backup & Recovery Gap Analysis

For organisations considering Covenco's services, we offer a complimentary **Backup & Recovery Gap Analysis**.

In a complete session we benchmark your current backup and recovery posture against our Enterprise Data Protection & Recovery Framework, identify gaps such as missing domain controllers, SaaS blind spots or untested runbooks, and provide a short, prioritised roadmap towards verifiable resilience.

To book your gap analysis, contact your Covenco account manager - or email: enquiries@covenco.com

About Covenco

Covenco is a modern private-cloud backup and recovery service provider, connecting data management services with robust IT hardware supply and support.

Drawing on over 35 years of experience, our team provides strategic expertise for Security and IT Leaders navigating complex data landscapes.

We support business leadership by addressing sophisticated compliance demands and delivering recovery strategies that ensure operational continuity while improving overall business resiliency. We provide world-class data protection solutions with a distinct advantage: unmatched speed in disaster recovery and hardware deployment.

Our UK data centres have over two Petabytes of customer data under management at any time, and we are fully ISO27001 and Cyber Essentials accredited for data security.

Contact Covenco

Covenco UK Ltd Head Office
Unit 4, MXL Centre, Lombard Way,
Banbury, Oxfordshire. OX16 4TJ
United Kingdom

Telephone: +44(0)1753 732000
Email: enquiries@covenco.com

www.covenco.com

covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

Gold Partner