‘Insurance-Ready’ Data Protection: From Compliance to Defensibility

Don’t let data protection fail when it matters most

Prepared by:

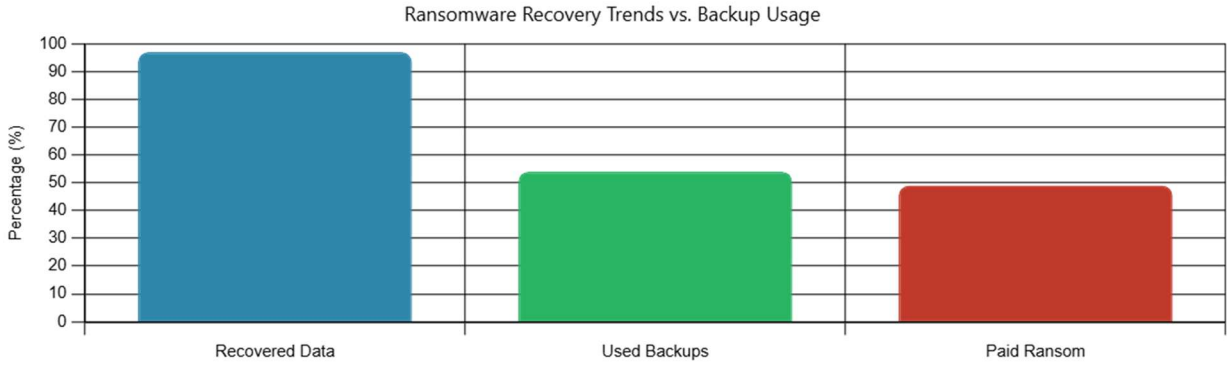
Executive Summary

Cyber insurance has undergone a fundamental shift. What was once a relatively simple underwriting exercise has become a rigorous examination of how organizations actually operate, secure, and recover their data. Across multiple major carrier applications, insurers now expect more than checkboxes—they expect **proof**.

Organizations are no longer evaluated solely on whether they *have* controls, but whether they can **demonstrate that those controls are effective, enforced, and will hold up during an incident or claim**. This change has elevated the importance of working with experienced data protection and security assessment partners such as Strategic Business Systems (SBS), who bring not just capability, but defensibility.

The New Reality: From Controls to Accountability

Insurance carriers are responding to an environment where cyber losses continue to escalate, ransomware attacks are constant, and claim scrutiny is intensifying. A ransomware event now occurs every few seconds globally, and outage costs can reach hundreds of thousands of dollars per hour. Against that backdrop, insurers are no longer willing to rely on unverified claims of data protection and security maturity.



Source: Sophos State of Ransomware 2025

With only half of ransomware victims actually able to recover from an attack using their backups, and the other half paying ransoms, who can blame insurers for asking these deeper questions? Can an organization prove their backups are immutable? Can it demonstrate that recovery procedures really work for all of their business critical data? Can it reconstruct events with logs, access records, and documented response procedures?

These are not theoretical questions—they are the foundation of underwriting, pricing, and claims decisions today.

This effectively creates an environment where **audit readiness is assumed**, even if it has not been formally declared.

The Risk of Getting It Wrong

The consequences of failing to meet this new standard are significant. Insurance policies rely heavily on applicant attestations. If controls are misrepresented or cannot be validated during a claim, insurers may rescind coverage, deny claims, or reduce payouts. In extreme cases, organizations may find themselves uninsured at the very moment they need coverage most.

"Organizations typically faced multiple operational gaps—an average of 2.7 contributing factors per attack."

Compounding this risk is a troubling industry reality: many organizations continue to rely on providers who have experienced breaches themselves (some multiple times!), who often depend on unvetted offshore labor, or who subcontract critical services to secondary and even tertiary subcontractors with little or no accountability, transparency, or insurance coverage of their own. From an underwriting perspective, that is not just a technical weakness—it is a very material risk factor. The latest Sophos report also calls out systemic operational gaps as being a major contributing factor that is leading to successful attacks.

It raises an uncomfortable but necessary question:

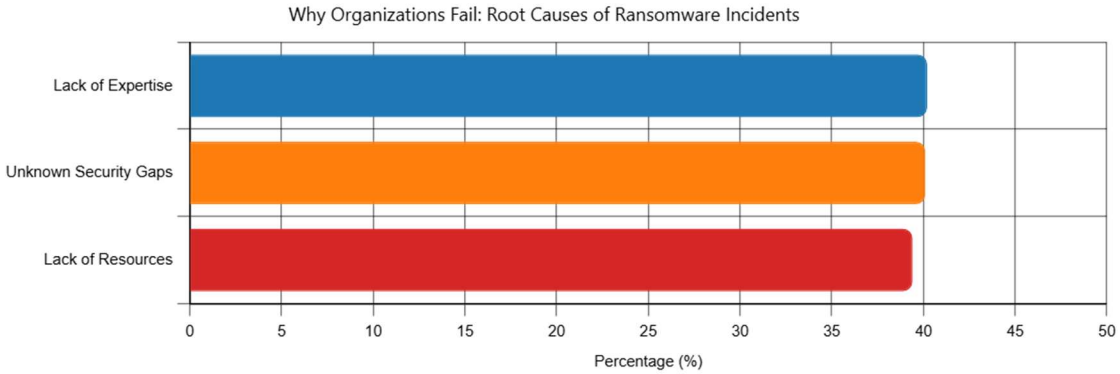
What would your insurance broker say if they fully understood how your data protection environment was being managed?

Why Expertise Matters: The SBS Difference

This is where experience and accountability matter. SBS operates in an entirely different class. Staffed exclusively with U.S.-based IT professionals on U.S. soil—including many veterans—with deep data protection and security discipline, and trusted daily within Department of Defense and Intelligence Community environments, SBS brings a level of rigor that few providers, big or small, can match.

Just as importantly, SBS maintains a perfect cybersecurity record, with zero breaches. That is not marketing language—it is the kind of operational proof that insurers are looking for.

In an industry where the large, well-known MSPs have suffered high-profile breaches, that distinction matters. And it matters even more to underwriters who are increasingly focused on **who is actually responsible for protecting critical systems and data**.



Source: Sophos State of Ransomware 2025

Note: Most ransomware incidents involve multiple contributing failures (an average of 2.7 per attack), highlighting that being compromised is typically the result of layered operational gaps—not a single point of failure.

The Role of Security Assessment and Data Protection Services

For both insured organizations and insurers, working with a trustworthy partner like SBS addresses a central challenge: moving from *perceived security* to *demonstrated security*.

From the insured's perspective, this begins with structured assessments that align directly with underwriting expectations. Rather than guessing at how to answer application questions, organizations can identify gaps, implement controls correctly, and ensure that their environment reflects not just best practices, but insurer expectations.

From there, it extends into execution. Controls such as multi-factor authentication, immutable backup infrastructure, and zero-trust access models must not only be deployed, but validated. Recovery procedures must be tested. Monitoring must be continuous. Documentation must be complete and defensible.

The difference is subtle but critical:
It is the difference between having controls and being able to prove they work.

Continuous Monitoring and the Importance of Evidence

Another key shift in the insurance market is the move away from point-in-time validation. Insurers are increasingly concerned with **ongoing posture**, not just how an organization looked at the moment an application was submitted.

That makes continuous monitoring and documentation essential. Events must be logged. Backup integrity must be verifiable. Recovery tests must be recorded and repeatable. Without this evidence, organizations face an uphill battle during claims investigations.

SBS provides this operational backbone—ensuring that data protection is not just implemented, but continuously validated and documented. This not only reduces risk, but strengthens an organization's position during underwriting and claims.

Supporting Insurers: Lower Risk, Better Outcomes

From the insurer's perspective, working with organizations supported by experienced partners like SBS results in clearer, more reliable risk profiles. It reduces uncertainty during underwriting and accelerates investigations during claims.

When an incident occurs, the difference becomes immediately apparent. Organizations that lack structure, or who rely on partners that treat IT service management as a commodity, will struggle to produce convincing evidence, reconstruct timelines, or validate controls. Those supported by disciplined data protection practices can deliver:

- Clear audit trails
- Verified recovery outcomes
- Demonstrated control enforcement
- Structured incident documentation

This reduces costs, shortens investigation timelines, and minimizes disputes—benefiting both insurer and insured.

Cyber Resilience: Beyond Insurance

At its core, this conversation is not just about insurance—it is about survival. Organizations must define what a "minimum viable company" looks like in the aftermath of a cyber event. How quickly must systems be restored? What data is critical? What can be lost, and what cannot?

Achieving that level of resilience requires a deliberate, structured approach. Best practices consistently point to five foundational steps:

- Protect all data using zero-trust principles and strong access controls
- Ensure data is recoverable through immutable, air-gapped backups

- Detect and investigate threats early through continuous monitoring
- Regularly test and refine recovery processes
- Maintain visibility into data risk and compliance exposure

These are not abstract recommendations—they are directly aligned with what insurers are now evaluating in every application and claim.

Conclusion

Cyber insurance is no longer a safety net for organizations that hope they are doing enough. It is a mechanism that rewards those who can **prove they are doing the right things, consistently, and can defend those actions under scrutiny**.

Organizations that continue to take operational risks will increasingly find themselves paying more in premiums, receiving less coverage, or facing denied claims. Insurers are simply no longer willing to absorb the risk.

Insurance readiness is not just about meeting requirements.
It is about proving them—and standing behind them when it matters most.

SBS ensures you can do exactly that.