CYBER INSURANCE ALIGNMENT

CHECKLIST FOR LEADERS

WE'RE HERE TO HELP.
LETS TALK

800-831-6660

www.datatel-systems.com

datatel
PAYMENT TECHNOLOGIES

Cyber Insurance Alignment

CHECKLIST FOR LEADERS

01 Understand Your Insurance Policy ☐

- ○ **Clarify the fine print:** Know exactly what your policy covers and what could trigger a denial.

Why this matters: Many claims are denied because leaders assumed coverage was automatic. Clarity prevents surprises when stakes are highest.

- ○ **Ask the hard questions:** Request clear answers from your insurer on what "properly secured" means in practice.

Why this matters: Terms like "adequate" or "properly implemented" are open to interpretation. Getting specifics now avoids disputes later.

02 Map Policy Obligations Against Standards ☐

- ○ **Connect the dots:** Compare your policy obligations with PCI, merchant agreements, and other regulatory requirements.

Why this matters: Insurance, compliance, and contracts often overlap. Gaps between them can leave your organization exposed.

- ○ **Spot the gaps:** Identify where your business standards fall short of insurance expectations.

Why this matters: Even small oversights can give insurers a reason to deny coverage. Spotting gaps early gives time to fix them.

datatel PAYMENT TECHNOLOGIES

Cyber Insurance Alignment

03 Involve All Departments

- [ ] **Finance:** Assess the financial exposure if coverage fails.

Why this matters: A denied claim could leave the company with millions in unplanned costs. Finance must know the risk upfront.

- [ ] **Legal:** Review agreements that add extra obligations.

Why this matters: Merchant service agreements may transfer full liability to you if standards aren't met. Legal needs to track this.

- [ ] **Operations:** Build compliance into daily workflows, not just annual audits.

Why this matters: Insurers look for ongoing discipline, not one-time checkmarks. Operations must make security part of a consistent routine.

- [ ] **Leadership:** Ensure alignment across teams so no one is working in isolation.

Why this matters: Breaches affect the entire business. Only leaders can create the cross-department coordination needed.

04 Strengthen Security Practices (as Strategy)

- [ ] **Raise the bar on access:** Treat strong login practices (like MFA) as a business standard, not an IT feature.

Why this matters: Weak access controls are one of the most common reasons insurers deny claims. Strong access is a leadership decision.

- [ ] **Protect business continuity:** Make sure backup and recovery planning is a leadership priority, tested and trusted.

Why this matters: A backup that doesn't work in a crisis can sink the business. Leaders must own resilience, not just IT.

- [ ] **Stay ahead of risks:** View patching and scanning not as "tech chores" but as part of your ongoing risk strategy.

Why this matters: Outdated systems are easy targets. Insurers may argue you failed in basic upkeep if you fall behind.

- [ ] **Pressure test your defenses:** Use testing and rehearsal (like simulations) as a way toto measure resilience and keep leadership accountable.

Why this matters: Testing reveals weaknesses before attackers do. It also proves to insurers that you are proactive, not passive.

datatel
PAYMENT TECHNOLOGIES

05 Validate Through Independent Review

- **Seek outside perspective:** Use third-party assessments to confirm your business is meeting expectations.

Why this matters: External validation adds credibility and catches blind spots internal teams may miss.

- **Build confidence:** independent validation strengthens your position with insurers, regulators, and customers.

Why this matters: An unbiased report makes it harder for insurers to dispute your compliance.

06 Strengthen Security Practices (as Strategy)

- **Make it cultural:** position compliance as part of everyday business, not a one-time event.

Why this matters: A culture of ongoing security lowers risk and reassures insurers.

- **Invest in people:** Ensure training and awareness is regular proactive, not reactive.

Why this matters: Employees are often the weakest link. Training reduces mistakes that could void coverage.

- **Stay current:** Treat insurer questionnaires as signals of what threats matter now and adjust accordingly.

Why this matters: Insurers update questions based on real attacks. Their forms show you where the risks are moving trending.

07 Strengthen Security Practices (as Strategy)

- **Plan ahead:** Don't just sign renewals; use them as checkpoints to test readiness.

Why this matters: Renewal season is the perfect moment to confirm policies, standards, and obligations are aligned.

- **Keep the receipts:** Maintain clear records of controls, policies, and reviews.

Why this matters: In a claim, documentation is your proof. Without it, coverage is at risk even if controls are in place.

- **Run practice drills:** Simulate an incident to see if you could prove compliance under pressure.

Why this matters: A dry run exposes gaps before a real crisis and prepares leadership to act quickly and confidently.

datatel PAYMENT TECHNOLOGIES

HOW DATATEL SUPPORTS LEADERS IN IMPLEMENTING THIS CHECKLIST

At Datatel, we recognize that a checklist is only as valuable as its execution. Many organizations struggle to align insurance obligations, compliance standards, and day-to-day operations. That's where we step in. With 27 years of expertise in secure payment technology, risk management, cybersecurity, and PCI compliance, Datatel helps leaders bridge the gap between policies and real-world practices.

As a PCI Level 1 Service Provider and PCI SSC Associate Participating Organization, we not only safeguard your payment ecosystem but also provide independent guidance to help ensure your obligations are met.

The result: You gain peace of mind knowing you can demonstrate alignment, mitigate risks, and secure coverage when it matters most.

WE'RE HERE TO HELP. LETS TALK

datatel
PAYMENT TECHNOLOGIES

800-831-6660 | WWW.DATATEL-SYSTEMS.COM

PCI & Cybersecurity Services offered in partnership with

SecuredNet