BTECH ENTERPRISE

Cyber Insurance Toolkit



Contact Us Today

BTECH ENTERPRISE

Cyber Insurance Policy Comparison Guide for Businesses

Use this guide to evaluate, compare, and confidently choose the right cybersecurity insurance policy.



First-Party Coverage
(Protects Your Business Directly)

Coverage Area	Carrier 1	Carrier 2	Notes
	✓ / ✗ / Optional	✓ / ✗ / Optional	
Breach Response Expenses			Covers forensics, notifications, credit monitoring, and legal support
Ransomware & Extortion Loss			Includes negotiation, ransom payments, and system recovery
Data Replacement & Recovery			Helps restore lost or corrupted business-critical data
Reputational Damage			Covers future lost income due to brand damage
Business Interruption & Recovery			Reimburses revenue lost during downtime caused by cyber incidents
Public Relations Support			Covers PR firm fees to manage fallout from a breach
Dependent Network Interruption			Covers losses due to outages at third-party providers
System Failure (Non-Cyber Causes)			Covers accidental IT outages unrelated to attacks
Bricking (Hardware Replacement)			Replaces devices that are unusable post-attack
Court Attendance & Investigation Costs			Covers employee time/support for legal or regulatory investigations

Third-Party Liability Coverage
(Protects You from Lawsuits)

Coverage Area	Carrier 1	Carrier 2	Notes
	✓ / ✗ / Optional	✓ / ✗ / Optional	
Privacy & Security Liability			Covers lawsuits from compromised customer/employee data
Regulatory Fines & Penalties			Pays government-imposed fines (HIPAA, GDPR, etc.)
Notification Costs			Covers costs to notify affected parties post-breach
PCI Fines & Assessments			Required for handling payment card data (PCI DSS)
Multimedia Liability			Protects against copyright, defamation, or online media claims
Technology Errors & Omissions (Tech E&O)			Crucial for IT providers or service firms with client-facing systems
Bodily Injury / Property Damage Triggered by Cyber Events			Covers damage resulting from cyber-related system failures

Cybercrime Coverage
(Covers Financial Theft/Fraud)

Coverage Area	Carrier 1	Carrier 2	Notes
	✓ / ✗ / Optional	✓ / ✗ / Optional	
Electronic Theft (Funds Transfer)			Covers wire fraud and banking transfer scams
Social Engineering / Impersonation Fraud			Protects against phishing and CEO fraud attacks
Invoice Manipulation			Covers forged or diverted invoices to/from clients or vendors
Cryptojacking			Covers hijacked systems mining unauthorized cryptocurrency
Payroll Redirection Fraud			Covers diverted employee pay deposits via impersonation
Telecom Fraud			Unauthorized use of phones or VoIP systems

Not Sure What You Need?

Most businesses don’t realize what their current policy is missing until it’s too late.

Use this checklist to identify gaps. Then talk with your MSP about how to better protect your business.

Want a Risk Assessment or Help Comparing Policies?

Ask your MSP for a Cyber Insurance Readiness Consultation.

JB Tech Enterprise

Choose someone who offers local cybersecurity support and proactive planning.

Disclaimer: This guide is intended for general informational purposes only and should not be considered legal or insurance advice. Coverage terms and conditions may vary between providers. Use this document to help organize your comparison process, but consult with a licensed insurance advisor or MSP to assess the best policy for your specific business needs.

BTECH ENTERPRISE

Smart Questions to Ask Your Cyber Insurance Provider

Not sure what to ask your insurance provider? Use these smart questions to uncover hidden exclusions, spot weak coverage, and make sure your policy truly protects your business.



Coverage Triggers & Conditions

1. What specific events must occur to trigger coverage? (Ex: Does employee error count? What about phishing?)

2. Are there exclusions for unsupported software (like Windows 10 after EOL)?

3. Do I need to notify you before making changes to our IT systems or providers?

4. What actions could void coverage or delay payouts?

Claims Process & Payout

5. How long does it typically take to process a cyber claim?

6. Will I have access to a breach response team or incident coach?

7. Are legal, PR, and forensic investigation costs included and under what limits?

8. Are ransom payments covered, and what's the limit?





Security Requirements

9. Do you require MFA across all accounts to issue or renew this policy?

10. Do I need to have Endpoint Detection & Response (EDR) tools in place?

11. What documentation do you require during a cyber insurance audit?

12. Are annual employee security awareness trainings mandatory for coverage?

13. Do I need to have a Security Incident Plan in place?

Third-Party Dependencies

14. If one of my vendors is breached, am I still covered under this policy?

15. What if the breach is caused by a remote employee's personal device?

16. Do you cover costs related to SaaS platform downtime or data loss?

17. Do I need to have employees sign a Bring Your Own Device Policy?





Renewals & Future-Proofing

18. Are rates expected to increase next year? What drives premium hikes?

19. Will this policy still be valid if I scale or open a new location?

20. How often are policy requirements updated and how will I be notified?

Not all policies are created equal.

The fine print matters, and your business's compliance posture today can make or break your ability to get reimbursed tomorrow.

BTECH ENTERPRISE

Cyber Risk Checklist



Is your business prepared to defend against cyber threats while your team is on vacation? Use this quick checklist to assess your risk level and spot gaps before cybercriminals do.

Staffing & Access

- [ ] We have a plan for monitoring systems while key staff are on vacation
- [ ] Temporary or fill-in staff have limited access to sensitive systems
- [ ] Remote employees are using secure, encrypted connections (e.g., VPN)
- [ ] Employee accounts require multi-factor authentication (MFA)

Phishing & User Awareness

- [ ] Our team has received phishing training within the last 90 days
- [ ] We've run at least one phishing simulation in the last 6 months
- [ ] Employees know not to click on suspicious links or unexpected attachments
- [ ] Staff are aware of summer-specific scams (travel invoices, fake vendors)

Device & Network Security

- [ ] All software and systems are up to date with the latest patches
- [ ] Antivirus and endpoint protection are active and monitored
- [ ] We use mobile device management
- [ ] Laptops and mobile devices are secured with strong passwords/passcodes

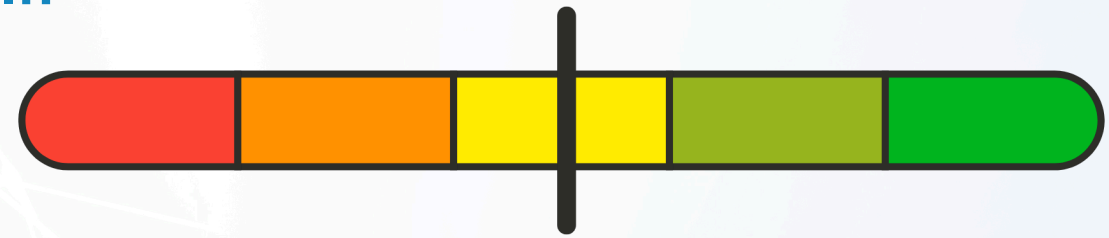
Backup & Recovery

- [ ] Data backups are scheduled, tested, and verified
- [ ] Backups are stored offsite or in the cloud
- [ ] We have a clear, documented recovery plan in place
- [ ] We know our estimated recovery time and cost in the event of an incident

Response & Support

- [ ] We know who to call if a cybersecurity incident occurs
- [ ] We have a plan for communicating with staff and clients during an event
- [ ] We use real-time monitoring or work with an MSP for active threat detection
- [ ] Our MSP or IT provider offers rapid response services (e.g., MDR, SOC)

Score Yourself:



0–9: High Risk.
Your business is vulnerable. It's time for a Cybersecurity Readiness Assessment.

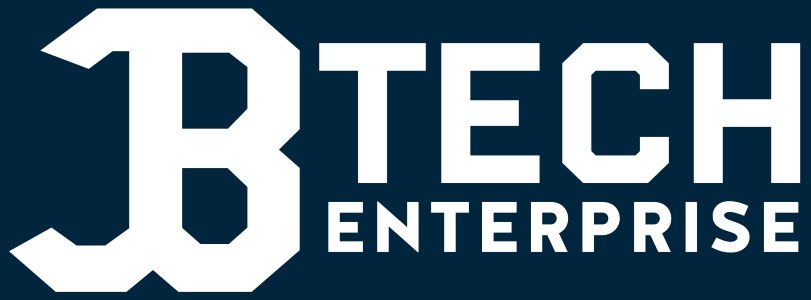
10–15: Moderate Risk.
A few small gaps could become big issues—act now.

16–20: You're Summer-Ready.
Well done! Stay alert and keep things current.

Need help fixing your weak spots?

Contact us for a free Cybersecurity Readiness Assessment and get a personalized action plan.

JB TECH ENTERPRISE


BTECH
ENTERPRISE