Cyber Simplified – Cyber Insurance Edition

NSB Cyber
No Steps Backward

5 Reasons Why an SMB Should Have Cyber Insurance

1. SMBs are a cyber criminals favourite Target

Many small to medium size businesses assume they're too small to be on a hacker's radar, that cyber-attacks only happen to big corporates. But that's exactly what makes them attractive.

With limited IT support and often little to no coverage on their cyber protection, SMBs are seen as low-hanging fruit. Whether it's a phishing scam or ransomware, attackers know what to look for, and its usually businesses just like yours.

Cyber insurance can help you bounce back when the unexpected hits – because it's not *if*, it's *when*.

2. The cost of a cyber breach can cripple your business

A cyber incident doesn't just shut down your systems. It can stop your business in its tracks. It affects your team, your customers, your reputation… and your bottom line.

The fallout typically includes:

- Business downtime and lost revenue
- Legal and regulatory costs
- Cyber experts to investigate and respond
- Customer notifications and compensation
- Long-term reputational damage

With the right policy, your insurer connects you with legal experts, incident responders, and communications specialists. That way you're not handling it alone when the pressures on.

3. It gives you expert support when you need it most

- Cyber insurance means you're not facing a cyber-attack alone. It means you've got the right experts on call, ready to respond, on your behalf and in your favour.

With the right policy, you get access to:

- Cyber Digital Forensics Incident Responders (the cyber technical experts)
- Legal and privacy experts
- PR and crisis comms support
- Help with data recovery and ransomware negotiations

And the best part? These response costs are covered. When you're under pressure, you don't want to be alone, or out of pocket more than you may already be.

4. It helps prove you're compliant and builds customer trust

Cyber regulations are tightening across all industries, not just for the corporate conglomerates of the world or those who hold highly sensitive data.

Today, customers, partners, and regulators all expect you to take security seriously. Having cyber insurance shows you're not just ticking a box. It shows that you're proactive, responsible, and ready for what's ahead.

It's not just about staying compliant; it's about earning trust.

5. It's not just IT's problem anymore, it's everyone's

A cyber-attack doesn't just hit your systems. It hits your entire business. From operations and finance to sales and leadership, the fallout is felt everywhere.

That's why cyber insurance is more than an IT decision. It's a critical part of your business continuity plan. It helps you respond fast, recover confidently, and keep your business moving… even (or especially) when things go sideways.

5 Things to Do When an Incident Occurs

1. Stay calm and don't touch anything

It's natural to want to act quickly, but resist the urge to shut down systems, delete emails, or "clean things up." Preserving digital evidence is critical, for the investigation, legal obligations, and your recovery.

2. Contact your cyber insurer immediately

Your insurer is your first call. They'll activate your policy's response support and bring in the right experts to the room. From dedicated cyber lawyers, digital forensics incident response consultants, crisis communications specialists, all ready to help.

3. Help the experts help you

The breach team will ask questions to understand what's happened. Be open, honest, and provide what's needed. The faster they can assess the situation, the faster they can contain the damage (because yes it can get worse post breach).

4. Communicate with care

Don't go it alone. Follow guidance from your insurer's crisis communication team and legal experts before speaking to customers, staff, or the media. Clear, consistent messaging helps protect your reputation and maintain trust.

5. Document everything

Keep a record of what happened, what actions were taken, and any communications sent. This supports your claim and may be required for compliance or regulatory reporting.

Thought we'd add a sixth, because this one is important … Learn and improve

Once the dust settles, take the opportunity to review what worked, what didn't, and where your systems or processes can improve.

Just because it's happened once doesn't mean it won't happen again. Especially now that attackers know you're a target.

Use the experience to strengthen your cyber resilience and take proactive steps to protect your business moving forward.

For more information, contact us via email on info@nsbcyber.com or visit www.nsbcyber.com

5 Questions to Ask Your IT MSP About Cyber Security

1. **What protections are in place to prevent ransomware or phishing attacks?**
2. **Do we have 24/7 monitoring and incident detection?**
3. **Are our backups secure, segmented, and regularly tested?**
4. **Can you provide reports or evidence of our patching, endpoint, and MFA status?**
5. **If we suffer a breach, what support will you provide and what won't you cover?**