


# What to gather before you apply for cyber coverage

HIGHSTREET
Insurance & Financial Services

Applying for cyber coverage goes faster when the answers are already in front of you. Your agent will ask how the business runs day to day, what data you store and what security you already have in place. **Use this guide to sit down with your team to get key answers, identify gaps and prepare for your cyber application.** Remember, even the questions you can't answer are useful — they show your agent where to start.

### Deterring cybercrime

- Do we verify fund transfer requests by phone before any money moves?
- What steps do we take to block unauthorized transfers?
- How do we confirm that vendor and supplier payment details are legitimate?
- Do we train our team each year on how to spot and prevent fraud?

### Multifactor authentication

- Does every account use multifactor authentication (the extra verification step after a password)? That includes employees, contractors and partners.
- Is it turned on for email, cloud systems, critical apps, admin accounts, virtual private networks and remote access?

### Encryption

- Are our emails, laptops and mobile devices encrypted?
- Does every device run antivirus and anti-malware software?
- Do we screen incoming email for suspicious attachments and links?

### Backups

- Do we back up critical data and systems at least weekly, with copies stored offline or on a separate network?
- Have we tested a restore to confirm the backups bring us back?

### Software updates and patching

- How quickly do we install security updates after they are released?
- Who confirms that an update actually installed?
- Do we know which of our internet-facing systems are due for a patch right now?

### Training and response planning

- Do all employees complete security training each year?
- Do we have a written incident response plan, and has anyone walked through it?
- Does the plan name who decides, who calls the agent and who talks to customers?

### Vendors and third parties

- Which vendors can reach our systems, our data or our customers' data?
- Do our vendors and service providers meet the same security standards we set for ourselves?
- If a vendor is breached, who tells us and how quickly?

### Artificial intelligence use

- Do we have a written policy naming which artificial intelligence tools employees may use?
- Does it say what company or customer data never goes into them?
- Do we know which tools our team is already using?

### Website tracking and privacy

- Do we know which tracking tools and pixels run on our website?
- Does our privacy policy name them?
- Who reviews the site when marketing adds a new tool and ensures those tools are updated and secure?

### Mergers and acquisitions

- Have we completed or considered a merger or acquisition in the past year?

### Operations outside the US

- Do we have operations or generate revenue outside the US?

### Sensitive data

- Do we collect or manage payment card data, health records or biometric data?
- How many records do we hold, and what is our yearly volume of payment card transactions?

### Losses and claims

- In the past five years, have we had any cyber incidents, extortion attempts, lawsuits or claims related to data or content?
- If so, how many, and what did they cost us?

### Security tools

- Do we use endpoint detection and response software, which watches laptops and servers for unusual behavior?
- What do we use to filter and secure incoming email?

Cyber risk keeps changing, and preparation is what keeps it manageable. Every question above is one your Highstreet agent can work through with you, and the gaps are the best place to begin.

Ready to go through the list? Your local Highstreet agent can help you **see possible**.

Talk to an agent >

Want to know what cyber coverage actually does? **Read the guide,** Cost of a Click 2026.

Get the guide >



HIGHSTREET
Insurance & Financial Services

©2026 Highstreet Insurance Partners Inc. All rights reserved.