

4 Claims Scenarios for Small and Medium Businesses

The following claim scenarios demonstrate how cyber risks might impact your business and how we can help.



► These Claims Examples are for illustrative purposes only.

The coverage examples included above are intended to show the types of situations that may result in claims. They shouldn't be compared to an actual claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.



1. Cyber Extortion

What Happened?: It's tax season, and you are finishing up your business tax filing. You get a Microsoft pop up on your screen: "Your computer is infected! Click on this website to scan your computer immediately." You click on the link and follow the instructions to call what you believe is Microsoft technical support. The cybercriminals take control of your computer and lock all of your data and systems access. To get your data back, you need to pay them four bitcoins worth over \$200k.

Lost Control: Without the data you can't operate as a business. You also need to complete your taxes.

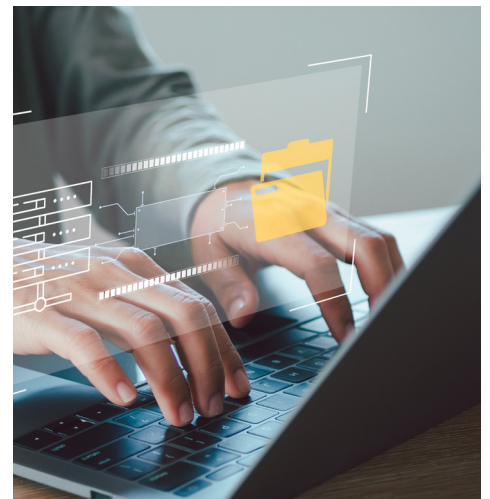
Now What?: Your Cyberboxx Business policy has cyber extortion event coverage to negotiate and pay a ransom. It will also cover Data Recovery to clean and restore your system. If client data was affected, you can rely on Legal Privacy Breach Costs.

2. Data Breach

What Happened?: You arrive at work and a friend sent you a news article about a data breach affecting the local municipality and its residents. You recall a contract you did last year for the city, where you had obtained resident data. The news is reporting that city suppliers could be to blame – and the city is conducting an investigation.

The Data Is Lost: Your Cyberboxx Business policy will complete a forensic IT review and determine if the data was compromised on your computer's systems. A legal review will be done to make sure you and your business are protected from any lawsuit. If needed, the costs associated with credit monitoring and a help line for affected residents will all be covered by your policy.

Now What?: Your insurance policy is helping you cooperate with the investigation and is retaining legal counsel to protect your business.





3. Online Fraud

What Happened?: A client reaches out and asks for a big order! To fulfill the order, you will need more material and you call your supplier to place an order worth \$15,000. You receive an invoice from the supplier for the order which mentions that they changed their banking information. You proceed to pay the invoice with their new bank details provided in the email.

Invoice Fraud & Payment Scam: A month later, the supplier follows up asking when you'll be paying their invoice. You had a quick chat with the supplier and let them know you paid the invoice to their new account as requested. Your supplier looked into the issue and confirmed that they did not change their payment details and that you were duped into paying cyber criminals via a fake invoice. Your business has now lost \$12,750 due to fraud and you still owe the supplier \$15,000. There goes your profits!

Now What?: Your Cyberboxx Business policy not only reimburses the stolen funds but also provides access to an expert vCISO consultation and forensic investigation to uncover how the incident occurred and help prevent similar events in the future.

4. Cyber Attack

What Happened?: You need new design templates for your business's sales materials. You find a website and download some free templates and unknown to you, the templates have keystroke logger malware embedded within them. This malicious software creates records of everything you type on a computer or mobile keyboard -- and later that day, you login to your business bank account.

Keylogging Malware: Equipped with your business's bank account password, the cybercriminals start sending small transfers of money to themselves. You change the password from the same device, and unknown to you, they are sent the new password. You change it again, they again get access. You call your bank and freeze all accounts.

Now What?: Your Cyberboxx Business policy covers the costs of system restoration and data recovery to remove the malware. It also covers for lost or stolen funds under online fraud coverage. You're back in business!



Now is the time to get protected and stay protected!

**Outsmarting
Cyber Risk
Together.**

To learn more please contact:
concierge@boxxinsurance.com