

Expert Tips to Protect Your Business

By Julie A. Rourke • VTC Insurance Group

"It's not a matter of IF, but WHEN..."

Every day, new stories break of the latest corporation to fall victim to unauthorized access of their computer network. Threats loom large and your manufacturing firm must be diligent to protect its data from cyber criminals.

Don't be fooled by the belief that your business is "too small" or that your networks lack the value hackers want — every company with employees and customers has valuable data. Names, birth dates, driver's license numbers, social security numbers, banking information are all "Personally Identifiable Information" — the most frequently exposed data.

Additionally, most manufacturers maintain online supply-chain relationships. Do you upload invoices or download purchase orders? Are you receiving or storing digital documents that contain privileged product information? These all represent the access points a skilled hacker looks for.

A trusted IT specialist is critical. Once you've vetted a potential firm and seen proof of their professional liability coverage, they can be a huge asset to protecting your data and that of your customers. These firms can assess your weaknesses and provide quality firewalls, anti-virus, malware and spyware software. They can help with password encryption and establishing back up protocols and advise on employee policies — all practices you should regularly revise.

Despite your best efforts, hackers are getting more sophisticated. Insurance can be the backstop to prevent financial crisis once a breach occurs. Policies vary, however, your insurance agent should be well versed in cyber liability policies, risk transfer, and fully understand the terms in the specific policy sold to you.



“Don't be fooled by the belief that your business is “too small” or that your networks lack the value hackers want — every company with employees and customers has valuable data.”

Transferring breach costs to an insurance company typically comes in two distinct forms:

- First-party expenses for your quantifiable losses, including breach response expenses and restoration of your network. It can also help with extortion demands, notification costs and even credit monitoring fees or regulatory fines. Some policies even offer lost revenue reimbursement of your business interruption.
- Third-party coverage involves liability or the obligation to pay for harm caused to others. This can include Privacy Liability suits for failing to keep private information

secure, virus/malware transmission, access issues, online libel, slander and more. When you purchase cyber insurance for your company, review the policy carefully for the triggers of coverage and important exclusions.

Even if you are a small manufacturer, recognize that you have substantial cyber-crime exposure and may need the help of a quality IT company to minimize your risks. Remember, it is impossible to eliminate your risk all together. However, by utilizing proper insurance coverage, you can avoid a financial disaster hitting your business in the wake of a cyber-attack. ⚙️



Julie A. Rourke is an account executive with VTC Insurance Group. She can be reached at 248-530-3273 or jrourke@vtcins.com.