A few years ago, Joe Palumbo, owner of Minneapolis-based Ice Dam Removal Guys, started getting angry calls about shoddy work. He was dumbfounded. There was no record of him servicing these people. Negative online reviews about his company’s ice removal services also began popping up from customers that weren’t his. After some digging, he learned that someone else was using his company’s name, causing immense confusion. Because he was a local leader in the ice dam removal business, he believes it was done maliciously. “He stole my company’s identity,” he says. “He was riding our coattails to get some of our business.”

Unfortunately, identity theft is a growing problem among small companies. In 2016, there were 82,000 reported cyber incidents among business of all sizes, says Craig Spiezle, executive director of the Online Trust Alliance, an organization that promotes online trust and security. Unreported incidences could bring this number closer to 250,000 a year. “You have to rethink what’s an incident,” he says. “Today’s threats have expanded exponentially, taking over social accounts, causing reputational harm, and affecting the identity of everything related to that business.”

In today’s world, breaches are inevitable, says Spiezle, and organizations need to be prepared. When such breaches happen, they can cause major problems, especially for a small business, says Jerry Thompson, senior vice president at Identity Guard, a Virginia-based business that helps prevent identity theft via a suite of security products.

Identity Guard provides several layers of protection with its new Breach Readiness product. First, customers conduct a forensic scan to find vulnerabilities in their computer systems. Hackers usually gain access to a company through phishing scams – an email is sent to a staffer who clicks on a link, allowing the hacker into the system – and then work their way into a network through these vulnerabilities. It is critical for owners to first find them and then patch them, says Thompson. Identity Guard has also created a document for its customers, which outlines best practices on how to prevent and handle a breach.

The idea is to prevent an attack, not simply react to one. “If a breach does occur, Identity Guard will help fix the problem. They provide identity-monitoring codes that alert employees if their personal information is used, and they also help people get their identity back by telling them how to deal with credit card companies or other affected services.”

Palumbo would have been well served by using other Identity Guard services, including social media monitoring. Independently, he hired a lawyer, sent a cease-and-desist letter, and used takedown notices to get content removed from the Internet. While the other company stopped impersonating his business, he knows there is always a danger of fresh attacks. “If you’re a leader, you’re always going to be a target,” he says. “I just need to be prepared for it.”

Identity theft doesn’t just happen to big companies; it’s a problem for small operations, too.

It’s a problem for small operations, too. After a data breach, lost time can increase risks to your company identity, employees, customers, propriety knowledge, and brand reputation. You won’t want to waste time wondering what to do. Get prepared with a breach readiness program from Identity Guard®. Benefit from a forensic scan for vulnerabilities in your network, a turnkey plan of action in case of a breach, and help recovering from a breach if it occurs.