CITIZENS STATE BANK
RIGHT BANK. RIGHT NOW!

Citizens State Bank
Newsletter Series

Understanding and Reducing Cyberrisks

"Manufacturers must strike a balance between progress and security," said National Association of Manufacturers board member Rick Schreiber in a recent statement. "Data analytics and the Internet of Things may spur the next industrial revolution, but with that comes increased exposure to cyberrisk. Manufacturers still have some catching up to do to adequately protect their data, customers, products and factory floors."

Data breaches can cause safety issues, negative publicity, lost productivity, and compromised personal and corporate data. This article explains the cost of data breach and outlines ways to help prevent attacks from inside and outside an organization.

Costs of data breach

Data breaches can cause safety issues, negative publicity, lost productivity, and compromised personal and corporate data. The average cost of a data breach in the United States has risen to a record high of $7.35 million, according to a 2017 study published by independent research group Ponemon Institute. That's an increase of 5% from the 2016 study.

The findings indicate that data breaches cost companies an average of $225 for each lost or stolen record. That includes $79 for direct costs incurred to investigate and resolve the breach, as well as $146 for indirect costs, including abnormal turnover of customers.

Preventive measures

Here are five proactive ways to minimize the risk of a breach:

1. Identify weaknesses. Many manufacturers own intellectual property — such as patents, designs and formulas — that may be targeted by thieves, including a dishonest person inside your organization. The use of automated equipment, cloud computing software, mobile devices and data-sharing arrangements also may provide other "ins" to hackers who want to exploit your company or its supply chain partners.
2. Turbocharge asset controls. Once you've identified at-risk assets, take steps to protect them. This includes encrypting electronic data; securing computers, smart devices and other IT equipment (including those used off-site); formalizing protocols for cloud storage and interfaced equipment (including secure disposal); and negotiating assistance from cloud storage providers in case of a breach.
3. Consider breach insurance. Most commercial liability policies don't cover losses for data breach or the cost of breach response. For this type of coverage, you'll need to purchase separate policies or addendums to your existing coverage. The amount of coverage needed depends on which assets are most at risk.
4. Train employees. The Ponemon study found that 24% of breaches were caused by negligent employees. So, train them about the latest scams and encourage the immediate reporting of suspicious incidents.
5. Establish a response team. Planning before a breach takes place can decrease the average cost of a data breach by about 12%, according to Ponemon. The response team can monitor for potential weaknesses, develop a response plan and conduct drills.

Audit must-have

Cyberthreats are a major risk manufacturers and distributors face today. Internal and external auditing procedures can help you evaluate and minimize the risks of data breach.

5 convenient locations:

Hudson
375 Stageline Rd.
(715) 386-9050

Elmwood
104 North Main St.
(715) 639-5411

Menomonie
1602 North Broadway
(715) 235-3164

Roberts
500 West Boulevard
(715) 749-3701

Woodville
140 South Main St.
(715) 698-2411