LEARNING FROM LOSSES

Protecting against cyber data extortion

When it comes to computers, we never really stop to think about how much we depend on them. But what if your access to that information was cut off? Customer accounts, payment information, inventory—you rely on being able to get to it at a moment's notice. There's a new disturbing trend where hackers are intentionally cutting off that access.

THE LOSS

A business offers its customers access to a proprietary system to help track preventative maintenance for their machinery. Suddenly, customers begin calling, saying they can't access their information. The company discovers a ransomware attack encrypted the data, and the hacker is demanding $125,000 to release the files. The company doesn't have data extortion coverage and paid the hacker directly to decrypt their customers' information. They also have to deal with a damaged reputation and tough customer questions about their data security.

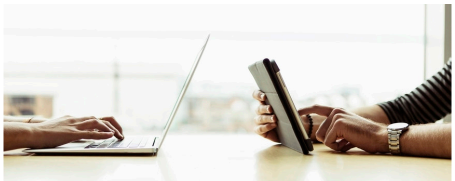
THE LESSON

Protection is possible. Front-end data security makes it harder for a hacker to get in. Other security and data backup upgrades might also limit the damages. In addition, data extortion coverage helps provide extra peace of mind.

PROTECTING YOUR DATA—AND YOUR CUSTOMERS

The good news is, there are things you can do to help protect your business and your customers' valuable information. Take a closer look at what you store and:

- **Identify sensitive data:** Look for Social Security and driver's license numbers, as well as any health and financial information.
- **Note where it's located:** Identify whether it's electronic or paper copy, how it's used, and whether you need it for your business. If not, consider deleting it.
- **Back-up data:** Ensure any data critical to your company's existence is secured and copied to a separate storage site.
- **Ask an expert:** Have a software/hardware security expert check your system for strong encryption and authorization protocols.



- **Immunize your system:** Make sure your antivirus package is current and able to block attacks.
- **Educate employees:** Teach workers to recognize and delete potential "phishing" scam emails.
- **Power-up passwords:** Require strong user passwords and regular resets to toughen security.
- **Avoid future problems:** If you meet an extortion demand, scan your database to make sure other malware hasn't been attached that could allow future attacks.

HOW SENTRY CAN HELP

At Sentry, we want to help you protect your business by providing the information and resources you need to help prevent losses before they happen. Remember, you can find additional safety resources through Sentry Connect®. Our Safety Services specialists are ready to answer any of your questions or concerns.

Give us a call at 800-443-9655.
Let's have a conversation about protecting your critical data.

The information contained in this document is of a general nature and is not intended to address the circumstances of any particular individual. IT IS DISTRIBUTED "AS-IS", WITHOUT ANY WARRANTIES. NO MEMBER OF SENTRY INSURANCE GROUP WILL BE LIABLE TO ANY PERSON OR ENTITY WITH RESPECT TO ANY LOSSES OR DAMAGES CAUSED, OR ALLEGED TO HAVE BEEN CAUSED, DIRECTLY OR INDIRECTLY BY THIS DOCUMENT, REGARDLESS OF WHETHER SUCH CLAIM IS BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE AND FOR PROPERTY DAMAGE AND DEATH) OR OTHER GROUNDS.

Property and casualty coverages are underwritten and safety services are provided by a member of the Sentry Insurance Group, Stevens Point, WI. For a complete listing of companies, visit sentry.com. Policies, coverages, benefits and discounts are not available in all states. See policy for complete coverage details.