Why Every Business, in Every Industry, Needs Cyber Coverage

By Chris Richmond
For WorkBoat Magazine

Today's marine industry relies on computers, smart phones and the Internet to operate and is just as vulnerable as any other industry for cyber attacks. An attack can have a significant impact on your employees, your customers, your reputation and can bring you serious financial loss. A cyber liability policy can provide risk management services useful to you before, during and after a data breach.

There are two important types of cyber liability to know about: First party and third party.

A first party cyber liability occurs when your own data is stolen. This can include your own employees' personal information or information about your customers. A cyber liability policy will provide credit monitoring services to assist the affected individuals which could help minimize the risk of identity theft. Included in the category of first party cyber liability are:

- **Funds Transfer Fraud** is an intentional, unauthorized instruction transmitted via email to a financial

institution to transfer funds. If your computer system is compromised, a hacker can have access to your banking information and initiate fraudulent electronic wire transfers.

- **Lost Business Income** due to cyber theft, (a hack or data breach), is not covered unless cyber coverage is in place. Your regular business insurance policy covers you for things like fire, theft and wind, but not anything cyber-related.

Third party liability coverage can provide protection for damage caused by your business to third parties due to a hack. This could be confidential client information that you store in your system. Coverage included in this category are:

- **Breach of Privacy**: A client's personally identifiable information has been accessed by an unauthorized party.
- **Misuse of Personal Data:** Personal data is stolen or misused and they suffer financial damages.
- **Transmission of Malicious Content:** Failure to stop the transmission of virus, malware or other malicious content.

Computers, smart phones and the Internet are as important as any other business tool. They also leave you vulnerable to losses. It is very easy to sit back and say your facility is too small and assume no one would ever want your data and think a hack could never happen to you. But since that is exactly what the hackers want you to say, best to consider adding cyber coverage to your insurance policy. Have a talk with your agent and learn more about this important coverage.

Why Do You Need Cyber Insurance?

By Karen Reed

This is another in our series of blog posts for business owners.

WHAT IS CYBER INSURANCE?

A cyber insurance policy can help protect your business from the fallout from cyberattacks and hacking threats. Having a cyber insurance policy can help minimize business disruption during and after a cyber incident, as well as potentially covering the financial cost of some elements of dealing with the attack and your recovery from it.

WHO NEEDS CYBER INSURANCE?

If your business stores any form of digital data, you need cyber insurance. These days, this is nearly every business.

WHAT SORT OF ATTACKS RESULT IN CYBER INSURANCE CLAIMS?

Cyber insurance claims can be triggered by many different incidents. Most common are ransomware, fund-transfer fraud attacks and business email compromise scams.

HOW MUCH DOES CYBER INSURANCE COST?

The cost of a cyber insurance policy depends on a number of different factors including the size of your business and its annual revenue. Other factors can include the industry in which you operate, the type of data your business typically deals with and the overall security of your computer network.

Everyone Who Uses a Computer Needs Cyber Coverage

By Chris Richmond
Originally Submitted to WorkBoat Magazine

A recent policy review with a client found an interesting update. The client, who distributes seafood, had reduced gross revenues. This was not surprising , given the downturn in the economy. What was surprising was a sharp increase in retail sales. Further discussion revealed that they had a growing online store with direct sales to consumers. They were in need of a cyber policy.

Whether or not you sell goods online, you really should consider a cyber policy. On daily basis, headlines in publications for every industry outline hacks, phishing schemes and other cyber crimes.

There are two important types of cyber liability to know about: First party and third party.

A first party cyber liability occurs when your own data is stolen. This can include your own employees' personal

information or information about your customers. A cyber liability policy will provide credit monitoring services to assist the affected individuals which could help minimize the risk of identity theft. Included in the category of first party cyber liability are:

• Funds Transfer Fraud. Funds Transfer Fraud is an intentional, unauthorized instruction transmitted via email to a financial institution to transfer funds. If your computer system is compromised, a hacker can have access to your banking information and initiate fraudulent electronic wire transfers.

• Lost Business Income. Lost business income due to cyber theft, (a hack or data breach), is not covered unless cyber coverage is in place. Your regular business insurance policy covers you for things like fire, theft and wind, but not anything cyber-related.

Third party liability coverage can provide protection for damage caused by your business to third parties due to a hack. This could be confidential client information that you store in your system. Coverage included in this category are:

• Breach of Privacy: A client's personally identifiable information has been accessed by an unauthorized party.

• Misuse of Personal Data: Personal data is stolen or misused and they suffer financial damages.

• Transmission of Malicious Content: Failure to stop the transmission of virus, malware or other malicious content.
Many liability policies come with limited cyber coverage but also they leave gaps in coverage. A stand alone cyber policy can cover these gaps and provide the insurance that a business needs today.

Do You Use 123456 as Your Password?

QUESTION: What were the top passwords leaked during 2020 data breaches?

We recently came across a new report looking at 275,699,516 passwords leaked during 2020 data breaches – it found that the most common passwords are incredibly easy to guess – and it could take less than a second or two for attackers to break into accounts using these credentials. Only 44% of those recorded were considered "unique."

If you cyber defenses have failed – or you have been breached by a hacker – cyber insurance can help you recover. Ask a member of the Allen Insurance and Financial business insurance team for more information about cyber coverage. Anyone who does business on the Internet really shouldn't be without it.

ANSWER: The most popular passwords from those 2020 data breaches included "123456," "123456789," "password," and "12345678." Read more about the report.

Tips for Avoiding Common

Holiday Cyberscams

For many of us, the holiday season is a wonderful time of year. Unfortunately, it can be especially profitable for cybercriminals. Because of the prevalence of online shopping, we almost always see a significant increase in cyberscams during November and December. To help you avoid becoming a victim of holiday cybercrime, here are some of the top scams to watch out for—and tips for avoiding them.

Shady Shipping Notices
During the holiday season, it's very likely that you will ship at least a couple of packages directly to your loved ones or have online purchases sent to your home. This makes the shipping notice scam a popular one for cyberscrooges. Here's how it works: The scammer crafts an email, purportedly coming from UPS or FedEx, notifying you of a problem delivering your package. To resolve the issue, you need only click on a link in the email message or open an attached invoice. Of course, doing so will install malware or ransomware on your computer or device.

Don't fall for it. Be particularly wary of emails claiming to come from any courier service. If you do receive a message like the one described above—whether you believe it to be legitimate or not—go to the website of the company you may have ordered from. You should be able to track your package from the retailer's site. Use the tracking number for the courier service that the retailer provides. You can also go directly to UPS.com or FedEx.com and obtain the delivery status there. Whatever you do, don't click on any links or download any attachments in the original message.

Eyebrow-Raising Refunds
This phishing scam is designed to steal your personal and financial information. Typically, an email claiming to be from

an e-commerce company like Amazon, eBay, or Overstock will say that something has gone wrong with your recent order. You will be prompted to click on a link in the message to obtain your refund. Unfortunately, if you do, you will be taken to a dummy website set up to look like a legitimate sender. There, you will be asked to fill out a form with your financial information to let the sender know where it can issue your refund.

Don’t fall for it. Again, to check the status of any order you may have placed, go to the company’s website directly (e.g., Amazon.com, eBay.com). If the company doesn’t offer the ability to check an order’s status, verify the transaction by calling the firm at a phone number that you know is legitimate.

Giveaways Galore

The gift card scam is seen year-round but more often during the holidays. These bogus offers are most commonly delivered by cybercriminals through social media, usually through a friend’s hacked account or a fake company page set up to look as if it’s legitimate. Appearing to originate from an entity like Best Buy, Ikea, or Whole Foods, the offer claims that the company is giving away hundreds or thousands of dollars in gift cards. But if you follow the instructions provided to obtain your gift card, you will likely be led to a phishing form that asks for your personal information.

Don’t fall for it. Remember, if something seems too good to be true, it probably is! If the post appears to come from a friend, call or text him or her to ask if it’s legitimate. In addition, be wary if the “official company page” looks a little off. Check how many followers the website has. The retailer’s authentic website may have hundreds of thousands or millions of followers. Further, a huge promotion such as the one described in the offer you received would also be listed on the retailer’s website, so check there directly or call the company’s customer service

number.

Website Vendors That Don’t Deliver

Many popular and novelty items may be sold out and on backorder until after the holidays. Or they may be hard to find from mainstream merchants altogether. So it’s not uncommon for consumers to search online for a less well-known vendor that may have the items. But beware! Another favorite holiday scam is staged through sketchy websites claiming to have hard-to-find items in stock. These sites trick you into paying for the items with no intention of delivering them. Often, these entities are based overseas.

Don’t fall for it. Search the Better Business Bureau website for customer reviews and the accreditations of merchants that are unfamiliar to you. In addition, because not all businesses are listed with the BBB, you might want to hunt elsewhere on the web for reviews posted by other consumers. If you can’t find much information on the vendor, stay away!

Still nervous? Below are additional tips to protect yourself from holiday scams:

• If possible, use credit cards for online transactions. If you fall for one of these scams and unknowingly hand over your debit card information, it’s easy for the cybercriminal to drain your bank account quickly. Purchases made with credit cards typically offer more consumer protections.
• If you’re uncertain about the legitimacy of a website, check its safety rating on Scamadviser.com or URLVoid.com.
• If searching for an item on a lesser-known merchant’s website, check for spelling and grammatical errors. If found, these mistakes are a red flag that the site is most likely based overseas—indicating a possible scam.
• Avoid online shopping or conducting any financial transactions

over an unsecure Wi-Fi network.

‘Tis the Season

With all the merriment and shopping during the holidays, the risk of inadvertently exposing your credit card or bank account details is very real. It’s important to take a step back and pay attention to the emails you’re receiving and the websites you’re using. By following the suggestions discussed here, you can help protect yourself against cyberscams so you can fully enjoy the holiday season.