AmeriTrust CONNECT

Defending Against Cyber Criminals

Businesses know how to defend against ordinary criminals. Door locks, safes, security cameras and more. Yet defending against cyber criminals is just as important given the risk to today's businesses. Cyber criminals commit crimes online by targeting computer networks and devices.

While ordinary crime levels may be relatively low, the cybercrime risk is rising each year. Just as you take ordinary precautions to effectively prevent crime at your business, it's important to take steps to defend your business from online thieves, too.

Here are three ways to reduce your risk of cyber-attack:

1. Safeguard Your Information

Cyber criminals often look for easy targets. For ordinary criminals, this might mean an unlocked door or open window. For cyber criminals, unsecured usernames, passwords and PINs allow easy access to your network or device, which can leave your business open to a damaging security breach, identity theft or financial crime.

If you fail to safeguard your vital information and passwords, it's like leaving the shop door unlocked at the end of the night. Protect your information from falling into the wrong hands:

- **Protect against deceptive imposter scams**: Never give out sensitive information to unknown persons over the phone. Vendors should never call to ask you for your password or PIN, even if there is a problem with your account.
- **Report suspicious texts and emails**: Cyber criminals may attempt to impersonate managers, employees, suppliers, vendors or even customers. Check the address or phone number, contact the party directly and report fraudulent messages to IT security.

2. Follow Best Practices

Just as law enforcement monitors the patterns of offline crime, cybercrime experts track the patterns of online cyber criminals. Both groups work to ensure the safety and frequently publicize the best practices to follow to avoid becoming a victim of crime.

Here are some current best practices regarding cybercrime prevention:

- **Use layered protection**: A password is one layer of defending against cyber criminals, but there are others. Multi-factor authentication is the latest method for reducing password hacking. With multi-factor authentication, a website or app that doesn't recognize your device or IP will text or email you a one-time code to verify your identity. A thief who only has your password won't be able to access your account thanks to the added layer of protection.
- **Monitor your activity**: Many financial institutions now offer fraud alerts, while other online portals offer regular security monitoring. Take advantage of these benefits and monitor your accounts for any unusual activities. If you do discover unauthorized transactions, report them immediately.
- **Stay alert for phishing attacks**: Phishing attacks by phone, text message or email can happen any time, but the volume spikes during holidays. Ensure messages are from a recognized contact and note that fraudsters sometimes use addresses very similar to the correct address. If you don't recognize a number of email address, don't open the message or click on any links and notify your contact directly.

3. Protect Your Business

The activities of cyber-criminals can often go unnoticed until the damage is severe. Protect your business by safeguarding your information, following proper security practices and ensuring you have the right cyber liability coverage.

Without liability protection, your business could experience lost data, decreased sales and reputational damages, as well as claims from customers or regulatory fines. With the increasing costs of a cyber-attack, it's more important than ever to ensure you have the cyber liability coverage your business needs.

CyberLock Defense Insurance is an one-of-a-kind cyber liability policy that offers comprehensive coverage at rates more affordable and more accessible than other cyber liability policies available. Coverage can help cover costs related to cyber-attacks and defending against cyber criminals, including privacy breach notification expenses, litigation, loss of income and regulatory fines and penalties.

Call AmeriTrust TODAY at (913) 339-5003 to request a quote.

Edition: 03/20

CyberLock Defense

AmeriTrust CONNECT

Getting Cyber Security coverage does not have to be a complicated process.

Achieving cyber peace of mind is now as simple as 1-2-3 with CyberLock Defense through AmeriTrust Connect.

1 OF-A-KIND SOLUTION

2 MINUTES

3 QUESTIONS

According to the FBI's 2019 Internet Crime Report, cybercrime losses reached $3.5 billion. (www.ic3.gov) The FBI Internet Crime Complaint Center also reported receiving 23,375 business email compromise/ email account compromise complaints in 2019 with losses accounting for $1.7 billion of the overall $3.5 billion in 2019. According to a recent SBA survey, 88% of small business owners felt the business was vulnerable to a cyberattack. (www.sba.gov)

CyberLock Defense coverage offers full access to your policy limits even for incidents to include cybercrime, social engineering, ransomware, and more. Should you ever experience a loss, a CyberLock Defense Specialist will help you develop a response plan and help with the claim.

To get this critical piece of protection for your business, call (913) 339-5003 or email cyberlock@ameritrustgroup.com.

CyberLock Defense

CyberLock Defense coverage offers:

BROAD COVERAGE
First and third party coverage options to address cyber extortion, breach of data privacy, contractual liability, copyright infringement and rogue employees

NO SUBLIMITS
The policy limit you select is the policy limit you get. If you select a $5M policy, you have full access to your $5M policy limit, even for incidents of cyber theft, social engineering loss, ransomware and more

ADDITIONAL COVERAGE
Business Interruption Expense and Extended Business Interruption coverage are included in your policy automatically, and at no extra cost

FLEXIBLE LIMITS
40+ industries, and policy limits from $500,000 to $10M

Edition: 03/20

AmeriTrust CONNECT

Cyber Defense Claims Examples

Cybersecurity is an area today's organizations can't afford to ignore. According to cybersecurity experts, systems access, customer data, business credentials and communications are all vulnerable. Plus, an attack can damage trust and harm your business. Explore these real cyber attack claims CyberLock Defense has covered.

Cyber Attack Claim #1 - Ransomware Attack

A mid-sized hospital network was the victim of a ransomware attack that caused an almost complete lockdown of its data. IT forensics had to quarantine the virus and ensure the unencrypted data and systems were operational.

The insured was required to rent extensive network and temporary equipment and route certain work, such as ER services and reading of x-rays and MRIs to other local providers. The insured incurred restoration of data costs, and needed privacy counsel to advise on HIPAA and other reporting obligations. Further, the insured experienced substantial business interruption losses.

CyberLock Defense covered losses:

- Privacy counsel: $30,000
- Forensic IT and data restoration: $55,000
- HIPAA notification expenses: $35,000
- Business interruption/loss income: $150,000

Cyber Attack Claim #2 - Fraudulent Funds Transfer Loss

A mid-sized real estate agency was in the business of buying properties, quickly restoring and updating the properties and "flipping" the homes for a substantial profit.

An administrative assistant received an email from the actual email address of the company's CEO, asking for $275,000 to be wired from the agency's account for closing costs of a new home. The assistant responded and had the funds wired as instructed. The instructions were fraudulent.

This fraud was the result of an email breach where the hacker had access to the CEO's email account and was able to set up a rule so that all emails on this topic went to a folder that only the hacker could see.

CyberLock Defense covered losses:

- Fraudulent funds transfer loss: $275,000
- Forensic IT analysis of email breach: $27,500

Edition: 04/20

CyberLock Defense

AmeriTrust CONNECT

Cyber Defense Claims Examples

Cyber Attack Claim #3 - Office 365 Email Data Breach

A small accounting firm had its email system breached via a phishing email that allowed the hacker to access an assistant's email and Office 365 account. The accounting firm handled may private client tax returns and exchanged financial information and draft returns via unencrypted messages.

A review of the assistant's Outlook account revealed that the hacker had access to the account for a period of 14 days during tax season. Hundreds of clients' personal and financial information were at risk.

CyberLock Defense covered losses:

- Privacy counsel: $40,000
- Data breach expenses: $30,000
- Notification cost: $10,000
- Credit monitoring costs: $10,000

Cyber Attack Claim #4 - Website Virus

A financial management firm had a virus infect its system. Any email that contained a link to the company's website was blocked by the recipient's spam filter. This was caused by a virus infecting the firm's website for the purpose of mayhem and chaos.

The firm had to notify all email recipients that the virus could have affected their computer or system. There is the potential for third-party claims if the recipients' systems were damaged.

CyberLock Defense covered losses:

- Data breach expenses: $40,000
- Notification cost: $5,000
- Potential third-party liability: Ongoing

Without a CyberLock Defense policy, these businesses would have been 100% responsible for paying the costs associated with these cyber attacks. Protecting your business from the threat of cyber attacks is critical.

CyberLock Defense Insurance is an one-of-a-kind cyber liability policy that offers comprehensive coverage at rates more affordable and more accessible than other cyber liability policies available. Coverage can help cover costs related to cyber-attacks and defending against cyber criminals, including privacy breach notification expenses, litigation, loss of income and regulatory fines and penalties.

Call AmeriTrust TODAY at (913) 339-5003 to request a quote.

Edition: 04/20

CyberLock Defense

AmeriTrust CONNECT

Do you worry about cyber security threats?

Cyber Security Coverage protects your business and your customers.

More small businesses are being targeted, attacks are more sophisticated, and criminals are getting away with bigger paydays. Cyberattack losses to small businesses almost doubled between 2017 and 2018, from $1.4 billion to $2.7 billion according to the FBI IC3 Report data. (www.ic3.gov)

To fully protect your business and your customers, it is important to have comprehensive coverage, with access to CyberLock Defense Specialists that can help you navigate the complex process of responding to a data breach.

CyberLock Defense coverage offers:

BROAD COVERAGE
First and third party coverage options to address cyber extortion, breach of data privacy, contractual liability, copyright infringement and rogue employees

NO SUBLIMITS
The policy limit you select is the policy limit you get. If you select a $5M policy, you have full access to your $5M policy limit, even for incidents of cyber theft, social engineering loss, ransomware and more

ADDITIONAL COVERAGE
Business Interruption Expense and Extended Business Interruption coverage are included in your policy automatically, and at no extra cost

FLEXIBLE LIMITS
40+ industries, and policy limits from $500,000 to $10M

Securing Cyber Coverage is Now as Simple as 1-2-3.

1 OF-A-KIND SOLUTION

2 MINUTES

3 QUESTIONS

To get this critical piece of protection for your business, call (913) 339-5003 or email cyberlock@ameritrustgroup.com.

CyberLock Defense

Edition: 03/20