CyberRisk

INFORMED RISK MANAGEMENT DECISION MAKING

LIBERTATE
an accretive™ company

Who's going to make the right call for you?

Our team of cyber professionals provide you with more than a quote, we give you the knowledge to protect your company.

MEET OUR TEAM

Libertate has collaborated with a team of experts to surround our clients with the best coverage, protection and tools.

Ross Warren

Vice President, Cyber

Ross joins the team with extensive insurance experience with a heavy focus on cyber security concepts incorporated into underwriting. Ross brings over 8 years experience as a production underwriter with Coalition and Ace Westchester, a Chubb company. His experience in the space provides our clients with an in depth perspective of the cyber market.

Paul Hughes

Principal

Paul Hughes has been working with the Professional Employer Organization (“PEO”) industry for over 30 years. He is a huge advocate for the PEO industry, having been a founding member of both NAPEO’s Workers’ Compensation Certification Board as well as Cyber Board.

Jeff Dorcely

Cyber Relations

Jeff is the lead on all cyber marketing. He prepares, packages and markets all client company cyber submissions for our PEOs. Jeff monitors quotes, performs comparisons, and prepares proposals, so our clients can choose the best option for their business. He also has extensive training in the utilization of the company's patented technology, RiskMD.

Gene McCulley

Owner of Domain Proactive

Gene launched his first company, StackFrame, in 2004. StackFrame is a developer of mobile and web-based applications and provider of IT services. Gene sold off StackFrame's Defense Division, responsible for the development of software for use in military training simulators, to focus on other areas. Gene's newest endeavor is DomainProactive, a cyber scoring platform that focuses on the PEO space.

CyberRisk

INFORMED RISK MANAGEMENT DECISION MAKING

We understand the Cyber eco system. Our proprietary PEO specific software is able to rank our PEOs' against their peers. Libertate Insurance Services understands the cyber vulnerabilities in the PEO industry, including 3rd party vendors.

What Makes us Different

- Our team of experts provides a comprehensive marketing plan for our PEOs
- Within 60 days of sending your submission to market we are evaluating and addressing potential issues
- We provide multiple options to fit you and your clients needs
- Monthly cyber security resources and tools to help protect your business

Cyber Risk Management Exclusive Add On

- 24/7 monitoring of your cyber profile
- Weekly cyber report with notices of changes
- Security scoring compared to other PEO organizations
- Help desk to assist with improving and resolving cyber issues issues
- PEO specific peer comparisons

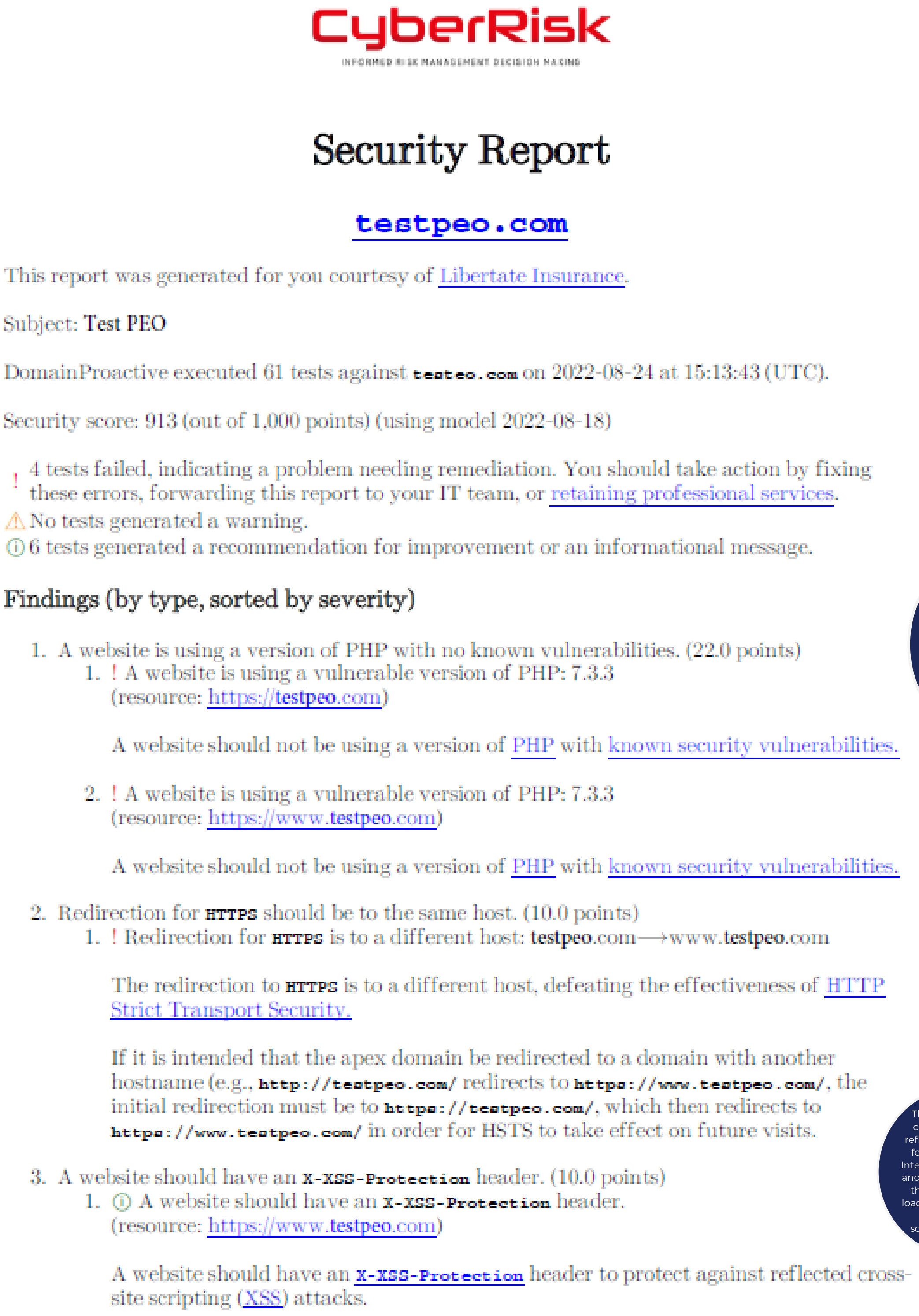
Every business's cyber risks are different depending on the type and complexity of its work. Our resources ensure that you are doing the due diligence necessary to understand and prepare for your organization's unique cyber exposures.

CyberRisk

INFORMED RISK MANAGEMENT DECISION MAKING

On top of what you will receive from our markets, our new security scoring model provides quicker intervals than other players in the market. We have tighten the overall approach. Our clients will receive daily reports, which include your security score, findings and assistance to remediating any issues. Our underlying data is compromised of system events, blank, blank and blank.

.



CyberRisk

INFORMED RISK MANAGEMENT DECISION MAKING

Security Report

testpeo.com

This report was generated for you courtesy of Libertate Insurance.

Subject: Test PEO

DomainProactive executed 61 tests against `testeo.com` on 2022-08-24 at 15:13:43 (UTC).

Security score: 913 (out of 1,000 points) (using model 2022-08-18)

! 4 tests failed, indicating a problem needing remediation. You should take action by fixing these errors, forwarding this report to your IT team, or retaining professional services.
⚠ No tests generated a warning.
ⓘ 6 tests generated a recommendation for improvement or an informational message.

Findings (by type, sorted by severity)

1. A website is using a version of PHP with no known vulnerabilities. (22.0 points)
    1. ! A website is using a vulnerable version of PHP: 7.3.3
       (resource: https://testpeo.com)

       A website should not be using a version of PHP with known security vulnerabilities.
    2. ! A website is using a vulnerable version of PHP: 7.3.3
       (resource: https://www.testpeo.com)

       A website should not be using a version of PHP with known security vulnerabilities.
2. Redirection for `HTTPS` should be to the same host. (10.0 points)
    1. ! Redirection for `HTTPS` is to a different host: testpeo.com⟶www.testpeo.com

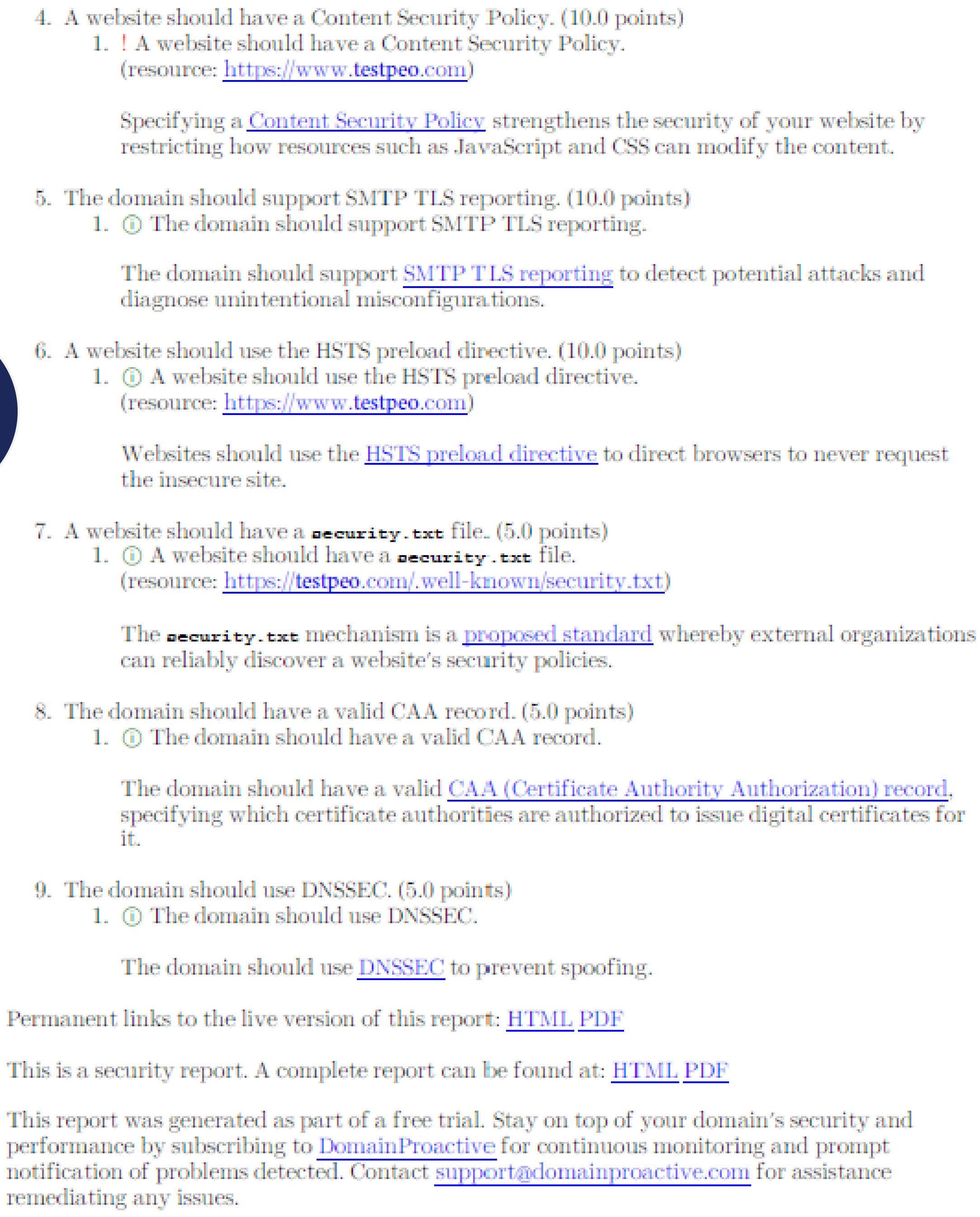
       The redirection to `HTTPS` is to a different host, defeating the effectiveness of HTTP Strict Transport Security.

       If it is intended that the apex domain be redirected to a domain with another hostname (e.g., `http://testpeo.com/` redirects to `https://www.testpeo.com/`, the initial redirection must be to `https://testpeo.com/`, which then redirects to `https://www.testpeo.com/` in order for HSTS to take effect on future visits.
3. A website should have an `X-XSS-Protection` header. (10.0 points)
    1. ⓘ A website should have an `X-XSS-Protection` header.
       (resource: https://www.testpeo.com)

       A website should have an `X-XSS-Protection` header to protect against reflected cross-site scripting (XSS) attacks.

Most PHP web applications share parts of code or scripts with other web applications. If the shared piece of code is found to be vulnerable, all the applications that are using it are also vulnerable

This header is used to configure the built in reflective XSS protection found in browsers (i.e. Internet Explorer, Chrome and Mozilla, etc) meaning that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks



4. A website should have a Content Security Policy. (10.0 points)
    1. ! A website should have a Content Security Policy.
    (resource: https://www.testpeo.com)

       Specifying a Content Security Policy strengthens the security of your website by restricting how resources such as JavaScript and CSS can modify the content.

5. The domain should support SMTP TLS reporting. (10.0 points)
    1. ⓘ The domain should support SMTP TLS reporting.

       The domain should support SMTP TLS reporting to detect potential attacks and diagnose unintentional misconfigurations.

6. A website should use the HSTS preload directive. (10.0 points)
    1. ⓘ A website should use the HSTS preload directive.
    (resource: https://www.testpeo.com)

       Websites should use the HSTS preload directive to direct browsers to never request the insecure site.

7. A website should have a `security.txt` file. (5.0 points)
    1. ⓘ A website should have a `security.txt` file.
    (resource: https://testpeo.com/.well-known/security.txt)

       The `security.txt` mechanism is a proposed standard whereby external organizations can reliably discover a website's security policies.

8. The domain should have a valid CAA record. (5.0 points)
    1. ⓘ The domain should have a valid CAA record.

       The domain should have a valid CAA (Certificate Authority Authorization) record, specifying which certificate authorities are authorized to issue digital certificates for it.

9. The domain should use DNSSEC. (5.0 points)
    1. ⓘ The domain should use DNSSEC.

       The domain should use DNSSEC to prevent spoofing.

Permanent links to the live version of this report: HTML PDF

This is a security report. A complete report can be found at: HTML PDF

This report was generated as part of a free trial. Stay on top of your domain's security and performance by subscribing to DomainProactive for continuous monitoring and prompt notification of problems detected. Contact support@domainproactive.com for assistance remediating any issues.

When HSTS is enabled, this means that even if a web user types in "http://" in a website URL, the browser would connect to the site using the "https://" protocol instead of the insecure HTTP.

Easy Quoting

Our easy quoting process and quick turnaround time provides our PEOs with multiple levels of coverage solutions.

Risk Purchasing Group Basic Coverage

This option is for client companies of the PEO. PEOs can sign up clients companies each month with this no underwriting model. Coverage is terminated when the client-PEO relationship ends. Price per client company: $15/mo to Liberate. The majority of PEOs on the program charge, at minimum, $25 per FEIN/per month. This program offers basic cyber coverage to client companies while also creating an additional revenue stream for the PEO.

1

Company Info

Legal name
Address
FEIN

Bulk Quoting

All we need is your payroll template. We can provide quotes to our existing clients in 24-48 hrs.

1

Company Info

Legal name
Address
*Payroll
Website

2

Experience

Verified loss history due at binding

*Estimated payrolls will serve to incept initial indication in lieu of projected revenues.

Custom Quoting

We provide easy quoting for our PEOs. The rating basis is on gross revenues. Libertate will interview each client to insure proper coverages are in place.

1

Company Info

Legal name
Address
Revenue
Website

2

Experience

Loss history
NAIC Code
Industry Comparable

3

Supplemental

Employee count
Security Assessment

*Additional information might be needed

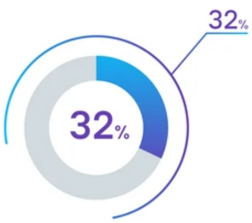
Client Company Coverages

In today's hyperconnected world nearly every business has some form of cyber exposure. Across industry lines, cyberattacks have surged in frequency and sophistication, resulting in a rise in cyber losses. To help protect your organization, it's important to understand the importance of cyber insurance. Libertate Insurance Services provides comprehensive Cyber Liability options that meet your unique organizational needs. We have access to multiple competitive markets. Our client company coverages are geared towards 100 employees or less in size.

Plan Type	Basic Risk Purchasing Group	Bulk Quoting	Custom
	No Limit	$50M Rev Limit	
Carrier Rating	A- (Excellent)	A+ (Strong)	Varies
Scoring Platform	N/A	Elpha	Varies
Retention	$1,000	$2,500	Custom
POLICY LIMIT	$250,000	$1,000,000	Custom
Business Interruption	N/A	$1,000,000	Custom
Cyber Crime	$10,000	$250,000	Custom
Data Restoration	N/A	$1,000,000	Custom
Data Subject Liability	N/A	$1,000,000	Custom
Dependent Business Interruption	N/A	$100,000	Custom
Extortion Loss/Ransomware	$10,000	Up to $1,000,000 $250,000 for $1,000 in premium	Custom
Hardware Replacement	N/A		Custom
Incident Response Expenses	$50,000 - includes legal, forensics and notification	$1,000,000	Custom
Media	N/A	$1,000,000	Custom
Network Security and Privacy Liability	$250,000	$1,000,000	Custom
Payment Card	$250,000	$1,000,000	Custom
Regulatory	$250,000	$1,000,000	Custom
Reputation Loss	N/A	$100,000	Custom
Utility Fraud	N/A	$100,000	Custom
Enhancements	N/A	Cyber ++ Endorsement	See Page 10

**Effective 1/1/2023*

AM Best noted that the top five insurers by premium—Chubb, Fairfax Financial, AXA XL, Tokio Marine and AIG—had a combined ratio of 102%.



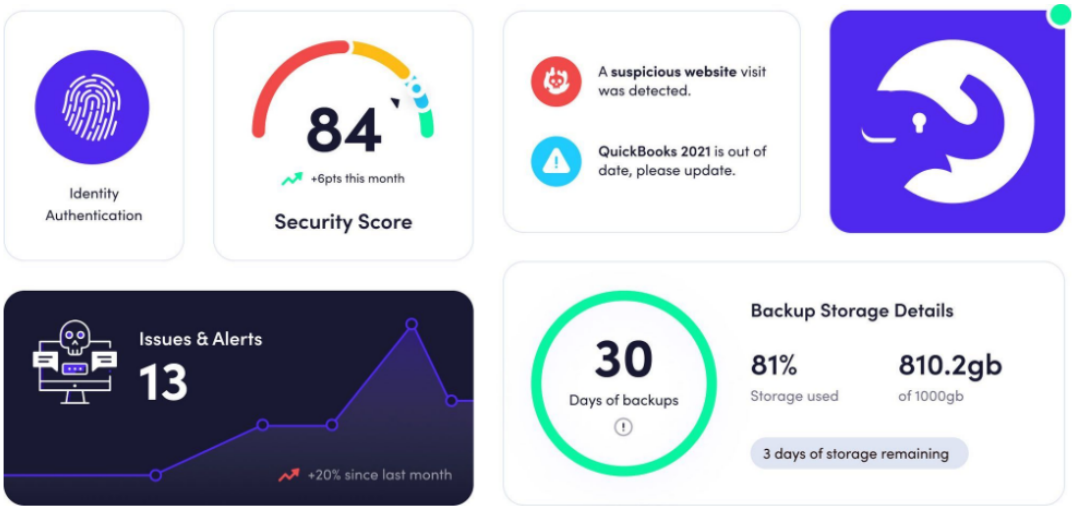
Industry data confirmed that ransomware attacks contributed to 32% of overall cyber-related losses in the first quarter of 2022.

ElphaSecure Cyber

ElphaSecure is a MGA/software provider that couples its service and software product with cyber insurance policy underwriting by an A- rated carrier. ElphaSecure is a very unique market that is highlighted it the coverage forms. The average client company premium is approximately $1k +/- and the application process is super easy. ElphaSecure will quote full portfolios with simple payroll data in days. In additional to cyber coverage, ElphaSecure also provides security software services through the installation of its product called ElphaWare. To qualify for full coverage, the insured would be required to install this product.

What You Receive

- An all-in-one digital defense that fits into your existing processes to manage your risk, with:
- A lightweight suite of features to defend against ransomware, social engineering, and more, all in real time.
- A user-friendly platform that allows you to keep control over your risk response and your business data.
- Automated updates and alerts when something goes wrong, and a human to help when you need it.
- Guaranteed security. Our software has been audited and validated by leading third-party security professionals.



A **suspicious website** visit was detected.

QuickBooks 2021 is out of date, please update.

Visit www.elphasecure.com

Custom Enhancements

Coverage	Custom	Others
Business Interruption & Extra Expenses	✓ See enhancements below[1]	✗ Sometimes
Contingent Business Interruption	✓	✗
Funds Transfer Fraud	✓	✗ Sometimes (sublimited)
Cyber Extortion	✓	✗ Sometimes
Computer Replacement	✓	✗
Bodily Injury & Property Damage	✓	✗
Pollution	✓	✗
Service Fraud	✓ See enhancements below[2]	✗
Network & Information Security Liability	✓	✓
Regulatory Defense & Penalties	✓	✓
Multimedia Content Liability	✓ See enhancements below[3]	✓
PCI Fines & Assessments	✓ No sublimit	✓ Sublimited
Digital Asset Restoration	✓ See enhancements below[4]	✓
Breach Response	✓	✓
Crisis Management & Public Relations	✓ See enhancements below[5]	✓

Enhancements	Custom	Others
Pre-claims assistance	✓	✗
Covers all prior acts	✓	✗ Sometimes
Systems failure[1]	✓	✗
Waiting period[1]	✓ As low as 1 hour	✗ 8+ Hours
Business services costs[2]	✓	✗
Cost of system upgrades[4]	✓	✗
Reputation Repair[5]	✓	✗
BYOD coverage	✓	✗
Social media / IoT coverage[3]	✓	✗ Sometimes
Cybersecurity apps	✓	✗

Coverage In Action

No organization is immune to the impact of cyber crime. As a result, cyber liability insurance has become an essential component to any risk management program. Cyber liability insurance policies are tailored to meet your company's specific needs and can offer a number of important benefits.

Data breach coverage

In the event of a breach, organizations are required by law to notify affected parties. This can add to overall data breach costs, particularly as they relate to security fixes, identity theft protection for those impacted by the breach and protection from possible legal action. Cyber liability policies include coverage for these exposures, thus safeguarding your data from cyber criminals

Business interruption loss reimbursement

A cyberattack can lead to an IT failure that disrupts business operations, costing your organization both time and money. Cyber liability policies may cover your loss of income during these interruptions. What's more, increased costs to your business operations in the aftermath of a cyberattack may also be covered.

Cyber extortion defense

Ransomware and similar malicious software are designed to steal and withhold key data from organizations until a steep fee is paid. As these types of attacks increase in frequency and severity, it's critical that organizations seek cyber liability insurance, which can help recoup losses related to cyber extortion.

Forensic support

In the wake of a cyber incident, businesses often seek legal assistance. This assistance can be costly. Cyber liability insurance can help businesses afford proper legal work following a cyberattack.

Legal support

Following a cyberattack, your organization will have to investigate to determine the extent of the breach and what led to it. The right policy can reimburse the insured for costs related to forensics and seeking out expert advice. Additionally, some polices can provide 24/7 support from cyber specialists, which is especially useful following a hack or data breach.

> *Cyber exposures aren't going away and, in fact, continue to escalate. Businesses need to be prepared in the event that a cyberattack strikes. To learn more about cyber liability insurance, contact us today at 321-217-7477.*

NetDiligence's 11th annual cyber claims study evaluated 5,797 claims arising from incidents between 2016 and 2020. Across the five years of claims data, ransomware accounted for 32% of all incidents affecting small to medium enterprises (SMEs). Hacking incidents were a distant second at 10%, and business email compromise followed at 9%.

40%

Last August, for example, American International Group (AIG), one of the country's largest writers of cyber insurance, announced that rates for its clients had increased nearly 40% globally and that it was tightening the terms of its policies to address increasing cyber losses."

Your renewal is a 365 day event that can now be tracked online at every moment due to the easiness of "Pen" (penetration) testing. In essence, how easy are you to be exploited available 24/7 to anyone that desires to understand an underbelly to attack.

Heightened business email compromise (BEC) risks

BBEC scams entail a cybercriminal impersonating a legitimate source within an organization to trick their victim into wiring money, sharing sensitive data or engaging in other compromising activities. According to the latest loss data from Advisen, BEC scams are among the most expensive types of social engineering losses, and they are on the rise—increasing 58% from 2015 to 2019. The median cost of a BEC loss is $764,000.

Be Prepared

Do not allow the "noise" surrounding the subject to confuse listening to what is important to change your corporate threat posture. Work with your insurance professionals to understand the different types of cyber coverage available and secure a policy that suits your unique needs. Carefully determine whether standalone coverage is necessary

VIGILANT INSURANCE REPRESENTATION

LIBERTATE

CyberRisk

INFORMED RISK MANAGEMENT DECISION MAKING

FLOWCODE

PRIVACY.FLOWCODE.COM

www.libertateins.com