Broker Insight Report:

How Insurance Oversights Can Lead to Devastating Claims Denials

CYBER RISK

Cyber attacks are a leading business risk.

You should never underestimate the potentially crippling effects of a cyber breach, or assume that your company is too small, too big or too protected to become a target. In fact, companies with less than $2B in revenues account for 88% of data breach claims.[9] The resulting compliance requirements and business interruption can be devastating, because SMBs are simply not equipped to survive such an event.

Shocking as it may seem, the source of a breach is often close to home. In fact, 25% of all cyber breaches are caused by the type of third-party vendors[10] you work with on a daily basis — your business partner, supplier or advisor. Sharing access to your network, even on a limited basis, and even with those you trust, opens you up to a potential cyber breach.

You may be putting your customer and employee data and intellectual capital at risk if you provide network access to any of the following partners:

- Payroll processing company
- Internet/cloud/phone service provider
- HVAC vendor
- Product supplier
- Inventory management firm
- Customer service provider

As many as

60%

of SMBs close their doors after a data breach, never to reopen again.[11]

26%

of breaches are caused by insiders,[12] whether inadvertently by human error or actively by a rogue employee. Have you trained your employees on how to respond to social engineering, spear phishing and ransomware attacks? 91% of successful data breaches started with spear phishing attacks.[13]

[9] Net Diligence 2017 Cyber Claims study
[10] Ibid
[11] Staysafeonline.com
[12] Net Diligence 2017 Cyber Claims study
[13] Trend Micro – http://www.infosecurity-magazine.com/news/91-of-apt-attacks-start-with-a-spear-phishing/

The Evolving Landscape

New cyber breach scenarios are constantly emerging, and they bring with them a variety of new claims. The fact that there's no industry-standard cyber policy language makes it a tremendous challenge to ensure your Cyber Risk insurance will really protect you.

> Just when you think you have your insurance figured out, a new situation arises or an event occurs that impacts your policy's terms and conditions. In this ever-changing environment, it's critical for your broker to understand your goals to negotiate and develop a policy that protects against your unique risks.
>
> **— Senior Vice President**

Four Truths about Cyber Risk Claims Denials

TRUTH #1

Claims can be denied due to your failure to act.

The top two reasons cyber claims are denied today are:

1. Late reporting
2. Failure to use the carrier's pre-approved vendors

Like all insurance claims, Cyber Risk claims must be reported "as soon as practicable" and within the policy period, or they will be subject to denial. Cyber insurers will have access to gold-standard vendors — including privacy attorneys, IT resources, and forensic, credit monitoring and public relations firms — and may require you to use these vendors under your policy agreement. Failure to do so will likely lead to claims denial, or erode your available limit due to other vendors' inexperience in managing such a claim.

TRUTH #2

Claims can be denied at the hand of a novice carrier.

With the rise in popularity of Cyber Risk insurance, more than 60 carriers now offer product coverage — some at very low prices. However, many lack real claims experience or a proven track record at managing and paying out cyber claims. Don't be the one to test a new Cyber Risk carrier's capacity to pay claims.

TRUTH #3

Claims can be denied due to coverage gaps, deficiencies and exclusions.

Lack of industry knowledge can lead to coverage disparities. Off-the-shelf Cyber Risk policies will not cover every data breach incident. Furthermore, not every cyber incident triggers Cyber Risk coverage. For example, spoofed emails that cause a company financial or securities loss are better insured under a crime policy. Ideally, asset protection policies, such as a crime policy, would work in tandem with your Cyber Risk policy to cover all your gaps, deficiencies and exclusions.

TRUTH #4

Claims can be denied because of generic coverage lines.

There is no standard Cyber Risk policy; however, these policies cover only intangible assets, such as data, and not the loss of money or securities resulting from a breach. Use predictive modeling to determine the potential impact of data loss and business interruption due to a cyber event; based on the results, you can decide which policy — and at what limits — will fit for your business.

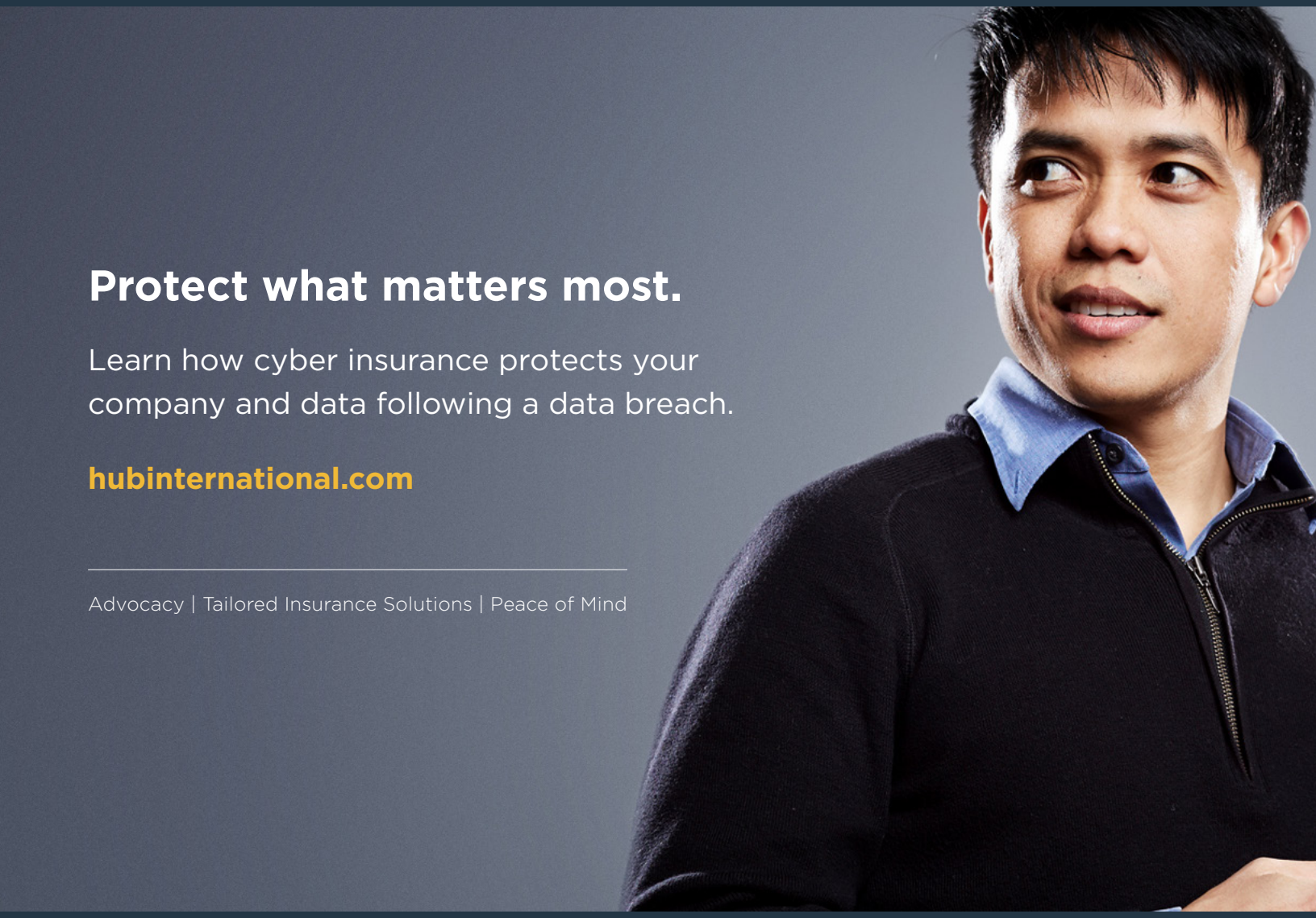
Real Cyber Risk Claims Stories

Phony email leads to costly data breach

An employee of one company received an email requesting copies of staff Wage and Tax Statements from what appeared to be his supervisor. He forwarded the forms. Several months later, company employees expecting tax refunds were informed by the IRS that their refunds had already been issued — albeit clearly not to them. The company spent considerable time and money investigating and determined that hundreds of records containing personally identifiable information had been compromised, and that the initial email had in fact been sent by a cyber criminal using a spoofed email address to impersonate the supervisor.

Ransomware attack holds computer system hostage

Employees of a business arrived one morning to find themselves locked out of the company computer system, which had been encrypted by ransomware. The cyber criminals responsible demanded $500 in bitcoins to unlock the system and return access.



Protect what matters most.

Learn how cyber insurance protects your company and data following a data breach.

hubinternational.com

Advocacy | Tailored Insurance Solutions | Peace of Mind

HUB