McGowanPRO

Professional Liability Insurance

Cyber-attacks and avoiding cyber insurance Fraud: What can you do?

Data breaches are becoming increasingly costly for companies. In fact, the average total cost of a data breach grew from $3.86 million in 2020 to $4.24 million this year. The increase in expenses coincides with a significant upswing in ransomware attacks—today's average weekly ransomware activity is 10.7 times higher than it was in June of last year.

Companies are now under renewed pressure to protect their networks. Finding the right insurance coverage ensures they can continue operations in the case of a cyberattack. With that comes the risk of—intentionally or unintentionally—committing cyber insurance fraud. Insurance companies recognize the increased risk and may require additional protections before approving cyber liability coverage.

This e-book will examine why cybercrime has increased and how companies can best protect themselves and avoid cyber insurance fraud.

Table of Contents:

What is causing the rise in cybercrime?

Cybercrime experts have dubbed 2021 the 'year of the outbreak,' but not for reasons related to the global pandemic. Instead, the cybersecurity landscape experienced wide-scale attacks that affected numerous organizations and individuals across the globe. These attacks are becoming a regular occurrence. According to a report from IBM, 83% of organizations had more than one data breach in the past year.

One potential reason is the massive move to digital transformation caused by the global pandemic. As many companies invested in cloud services and remote working capabilities for the first time, they opened the door for malicious attacks.

What does this have to do with cyber insurance?

Today, insurers will ask questions about a company's cybersecurity measures. These can include questions about:

- Multi-factor authentication (MFA).
- Encryption.
- Vulnerability management.
- Employee security awareness training.

MFA, in particular, is already being used by many companies and even individuals to access everything from their social media to their banking accounts. It requires the user to provide two or more verification factors to access online resources. These can be:

- Known information, such as passwords.
- Inherent/biological traits, such as a fingerprint.
- Possessions, such as a scannable card.

Is multi-factor authentication now mandatory?

The reality is that even if you generate strong, unique passwords, hackers will have a multitude of methods to break into your organization. These can include but are not limited to:

- **Phishing:** People at your company are contacted via email, telephone, or text message by someone posing as a legitimate institution. Employees are then convinced to voluntarily hand over sensitive data that could put the company at risk.
- **Extortion:** The company receives a threat of attack or is attacked, after which the attacker will demand money or some other response to stop the attack.
- **Keystroke logging:** Malicious software is secretly installed on a company's network, after which it tracks personal and sensitive information.

Instead, companies looking to acquire cyber insurance should immediately begin overhauling their networks to include MFA. Implementing additional authentication methods like MFA can dramatically reduce a hacker's ability to access your business.

Preventative measures such as an SMS code sent to a phone have the power to stop targeted attacks, bulk phishing attacks, and automated bots. On-device prompts provide another level of safety. It quickly becomes clear why insurance companies are mandating that prospective clients implement MFA in their network.

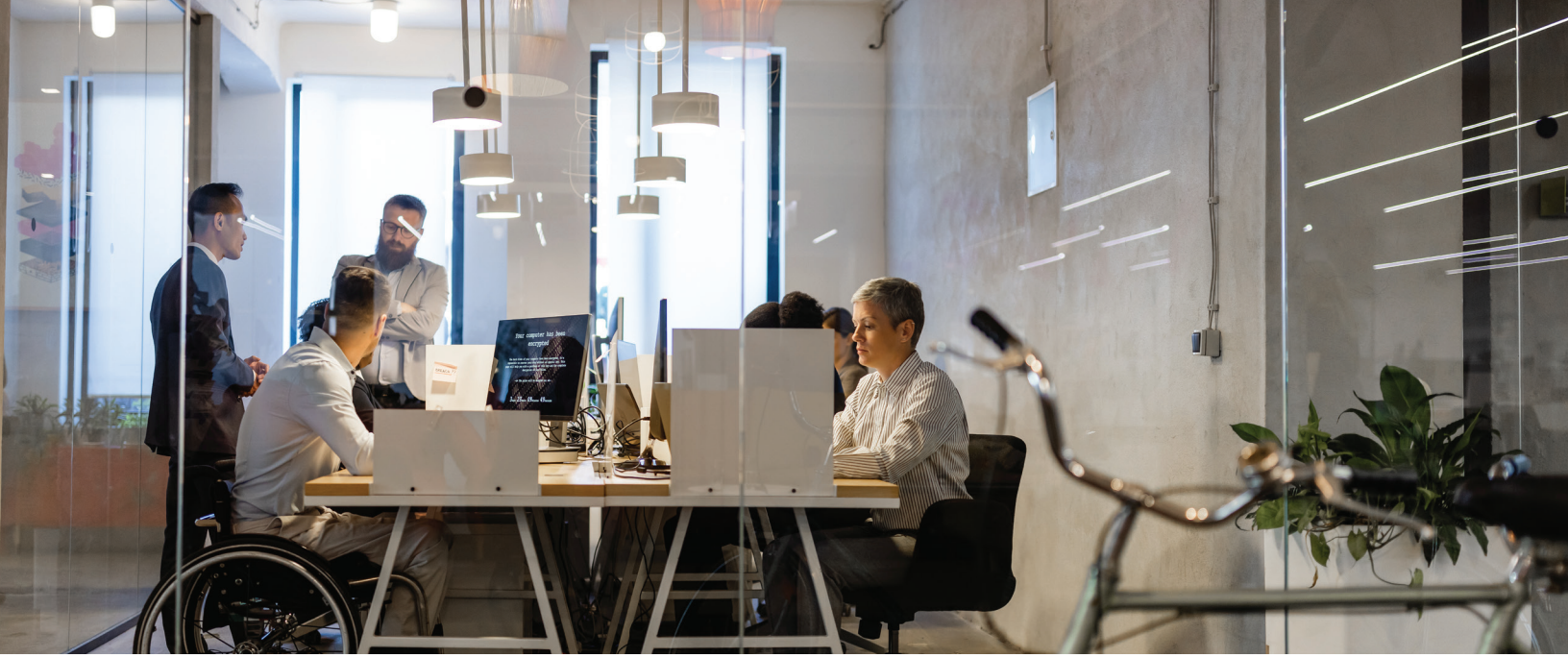
Where does cyber insurance fraud come in?

Implementing MFA can be complicated and costly, especially in large, global companies. Unfortunately, delaying implementation can have significant consequences—especially regarding insurance coverage. International Control Services (ICS) suffered a cyberattack in May, just a few days after being approved for cyber insurance.

The breach cost the company millions of dollars and resulted in a class action lawsuit served by its clients. Then, in July, ICS's cyber insurance provider filed to nullify their policy. It came to light that, while investigating the cyberattack, the provider had discovered ICS had allegedly misrepresented its implementation of MFA. ICS had only used MFA to protect its firewall and had not implemented it to protect any other digital assets—as was required by their insurance policy.

The provider filed to declare the insurance contract null and void, rescind the policy, and ensure it had no duty to help ICS in its insurance claim. It argued that if the provider had known about ICS's alleged misrepresentation and omission, it would never have approved the policy.

Because of its cyber insurance fraud, ICS not only endured a costly cyberattack that angered its clients, but the fraudulent claims made to secure cyber insurance compromised its relationship with its insurance provider.

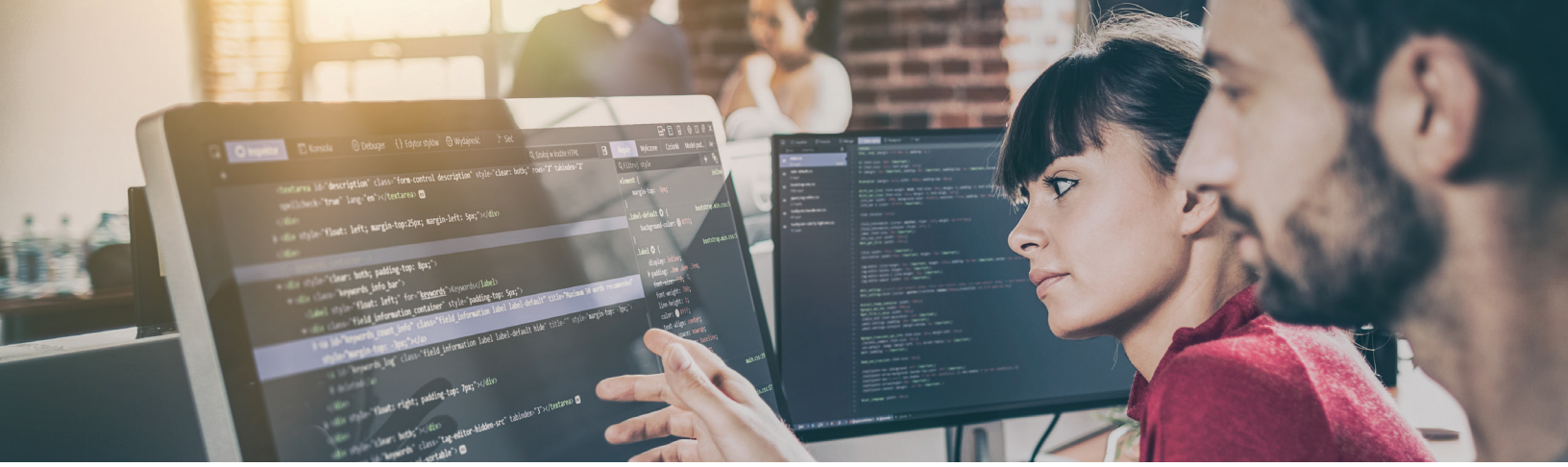


How can you protect yourself against claim denial?

The ICS case and subsequent court filing may leave a lasting impact on the cyber insurance fraud landscape. It might even affect how insurance companies deny claims based on misrepresentation. However, it may help companies identify pitfalls in their protections and require them to research how to prevent the same thing from happening to them.

There are a few ways to protect yourself from claim denial:

- **Be completely factual in your insurance application.** While there may be a temptation to bend some answers and avoid the arduous, expensive process of meeting compliance goals, the ICS case shows that the consequences of cyber insurance fraud can be severe. Providers evaluate applications thoroughly, and if they find any inaccuracy, act upon it immediately. Misrepresenting your insurance application or not giving a complete picture of your business's network is one of the fastest ways to a claim denial, leaving companies vulnerable to attack.
- **Thoroughly understand the policy requirements.** Ensure your team has read the terms and conditions, clarified any confusing terminology, and reviewed the requirements multiple times. If the insurer finds you are missing critical details, they will likely deny the application.
- **Understand your network.** Claim denials are not just caused by misrepresentation; they can also come from ignorance. A wrong answer in the application may invalidate it or leave you with gaps in your coverage. Many insurance documents are incredibly technical and have only become more so in recent years. Having someone on your team who thoroughly understands your network and security is crucial to ensure you submit a factual application.
- **Receive help from security experts.** Your IT team is busy with the day-to-day operations of your technology, making it challenging to shift attention to upgrading network security and meeting compliance. Instead, a security expert or an IT support company can help, easing the pressure on your team and ensuring you satisfy compliance requirements.



Moving forward

The possibility of a claim denial is nerve-wracking for businesses already concerned about the eventuality of cybercrime. However, honesty during the application process, knowledge of the network, solicitation of experts, and careful attention to detail will minimize the likelihood of claim denial.

The effort required is worth it, as companies are not just shoring up their defenses but also making themselves eligible for insurance that protects against cybercrime's worst effects. Ultimately, going the extra mile is better than experiencing a cyberattack without adequate coverage. Firms of all sizes should identify gaps in their current plan, ensure they meet compliance requirements, and be ready to contact experienced security professionals when necessary.

If your company suffers a cyberattack, ensure you have industry-leading coverage that assists you during data security and privacy breaches. Contact us today to find the right policy for your company's needs.

McGowanPRO
Professional Liability Insurance

Contact us:

L Squared Insurance Agency
2430 Camelot Ct
Grand Rapids Mi 49546

Phone: 616-940-1101 | Fax: 616-940-1196
Info@L2Ins.com