




digital hands® | GET THERE FIRST™

A Guide to Cyber Insurance: Prevent Claim Denial and Ensure Protection



The latest trends in cybersecurity are concerning—ransomware attacks have skyrocketed, cyber threats have become more sophisticated, and an exponentially evolving attack surface has made cybersecurity leaders anxious.

But they're not the only ones—since insurers bear much of the cost of damages, they, too, have become increasingly nervous about evolving cyber threats.

As the risks continue to grow, insurers have raised premiums and made it difficult for you to make a claim after a data breach. According to insurance broker Howden Group, global insurance pricing has increased by 32% as insurers grapple with the surge in cyber risk.¹

¹ Global cyber insurance pricing increases 32% as insurers grapple with the changing face of cyber risk; [Howden Group](#)

This points to a grim possibility—with more stringent policies in place, should organizations like yours worry about denied cyber insurance claims? In the event of a security breach, you could be forced to pay the cost of damages yourself.

While it's important to invest in coverage, you have to do your due diligence to ensure that your policy delivers in the worst-case scenario—or risk bearing the full responsibility and cost of all damages.

This Cyber Insurance Guide dives into:



**The rising threat
of ransomware
and its impact on
cyber insurance**



**Rising insurance
premiums and the
high cost of claim
denial**



**How to improve
your cybersecurity
posture to ensure
insurance payout**



RANSOMWARE: THE CAUSE AND CATALYST OF CYBER INSURANCE ANXIETY

It's undeniable that ransomware is one of the biggest threats to organizations today. One of the largest ransomware payouts was made last year by insurer CNA Financial at a reported \$40 million². Meanwhile, computer giant Acer Inc. faced a record-breaking \$50 million demand from a ransomware group that held stolen corporate data³.

Security experts at Cybersecurity Ventures predict that ransomware will cost an annual \$265 billion loss by 2031 with a **new attack every two seconds** as threat actors refine their malware payloads and extortion tactics⁴.

Double-extortion attacks, in particular, allow ransomware gangs to maximize damage and increase ransom payout from organizations. In the first extortion, hackers encrypt the victim's data and copy it onto their servers, forcing victims to pay to release that data. The cyber cartel then keeps the copied data for future extortions⁵.

Analysts at Risk Placement Services note that double extortion has become a substantial contributor to cyber claim severity in their 2021 US Cyber Market Outlook report⁶, triggering alarm bells for insurers. Meanwhile, risk management firm CyberCube cautions that these attacks will happen more frequently, with hackers preying on sensitive data such as those found in healthcare and financial services⁷.

The Cost of a Ransomware Attack

- **\$170,404**
Average ransom paid by a mid-sized organization
- **22 days**
Average length of business downtime after a ransomware attack in the US
- Only **11%** of organizations successfully recover data within 72 hours of a cyberattack

² One of the biggest US insurance companies reportedly paid hackers \$40 million ransom after a cyberattack; [Business Insider](#)

³ Acer Faced With Ransom Up To \$100 Million After Hackers Breach Network; [Forbes](#)

⁴ Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031; [Cybersecurity Ventures](#)

^{5,7} Enterprise Ransomware: Assessing the future threat and what it means for (re)insurers; [CyberCube](#)

⁶ U.S. Cyber Market Outlook; [Risk Placement Services](#)



RANSOMWARE HAS CHANGED THE GAME FOR CYBER INSURANCE

As damages from ransomware grow exponentially, insurance companies grow more fearful. Ransoms, business interruption losses, legal fines, and damage mitigation can cost millions—and **insurers are no longer willing to bear the costs.**

Insurers are now scrutinizing their cyber policies for new customers and renewals to include more stringent limits and restrict policy terms with additional exclusions to account for increased risk⁸. Insurer American International Group, Inc (AIG) announced in August 2021 that they were cutting their cyber limits to address the rising threat of ransomware, even as premium prices soar⁹.

Insurers who previously issued \$5 million cyber liability policies in 2020 have reduced their limits to between \$1 million and \$3 million in 2021, even on renewal¹⁰. Insurers are also increasingly discerning with their payouts—some are asking policyholders to pay half of the ransom amount, while others are **refusing to pay at all.**



Cyber insurance pricing in the US **increased 96%** year-over-year in Q3 2021

⁸ Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market; [U.S. Government Accountability Office \(GAO\)](#)

⁹ AIG is reducing cyber insurance limits as cost of coverage soars; [Reuters](#)

¹⁰ U.S. Cyber Market Outlook



DENIED INSURANCE CLAIMS: WHAT COULD THEY COST YOUR ORGANIZATION?

With insurance companies limiting payouts and making it difficult to file a claim, organizations are quickly realizing they are not as financially protected as they thought.



01 | Insurance penalties

Insurance policies require specific contractual terms and conditions be met; failure to comply can be grounds to deny or significantly reduce claim payments. After an attack, insurers typically hire costly forensic experts to verify the claim amount and investigate the cause of the breach.

If investigators discover that the data breach was caused by a lapse in your security, not only will insurers deny the claim, but you may be asked to bear the costs of these experts' services.



02 | Legal expenses

Recent reports estimate that the legal claim for a large company following a breach average to \$1.7 million¹¹. However, if the insurance claim is denied, companies can suffer additional costs from an expensive and lengthy legal battle with the insurer.

The pharmaceutical giant, Merck, suffered \$700 million in damages after the 2017 NotPetya ransomware attack and had to initially pay the full amount out-of-pocket when insurers denied their claims. Food conglomerate Mondelez International, also hit by NotPetya, sustained over \$100 million in financial loss when their claims were denied by Zurich Insurance. Both companies suffered additional legal costs when they took their insurers to court.

While Merck finally won their legal dispute five years after the attack, Mondelez's case is still ongoing and could take years to resolve¹².



03 | Regulatory fines

If a ransomware attack against your organization leads to the successful exfiltration of sensitive data, **lawsuits won't be your only concern**. You'll also face heavy fines from failure to meet data compliance standards such as **GDPR (General Data Protection Regulation)**, **HIPAA (Health Insurance Portability and Accountability Act)**, and **CCPA (California Consumer Privacy Act)**.

Health insurer Premiera Blue Cross's 2020 data breach set a grim example when it was fined a whopping \$6.85 million—the second largest ever HIPAA penalty. Investigations revealed that the company failed to conduct a comprehensive risk analysis and implemented insufficient hardware and software controls, which ultimately led to hackers seizing the health information of over 10 million customers¹³.

With the possibility of a denied claim causing so much devastation to your organization, it's crucial you implement protective solutions to avoid a worst-case scenario.

¹¹ Cyber Claims Study 2021 Report; [NetDiligence](#)

¹² Merck's \$1.4 Billion Insurance Win Splits Cyber From 'Act of War'; [Bloomberg Laws](#)

¹³ OCR Imposes 2nd Largest Ever HIPAA Penalty of \$6.85 Million on Premiera Blue Cross; [HIPAA Journal](#)



YOU CAN STILL AVOID CYBER INSURANCE CLAIM DENIAL

To avoid the risk of claim denial (as well as minimize the cost of insurance premiums), you must improve your risk profile by taking the proper precautions and implement proactive security solutions to perform your due diligence.



1 in 3

organizations are not prepared to deal with ransomware threats

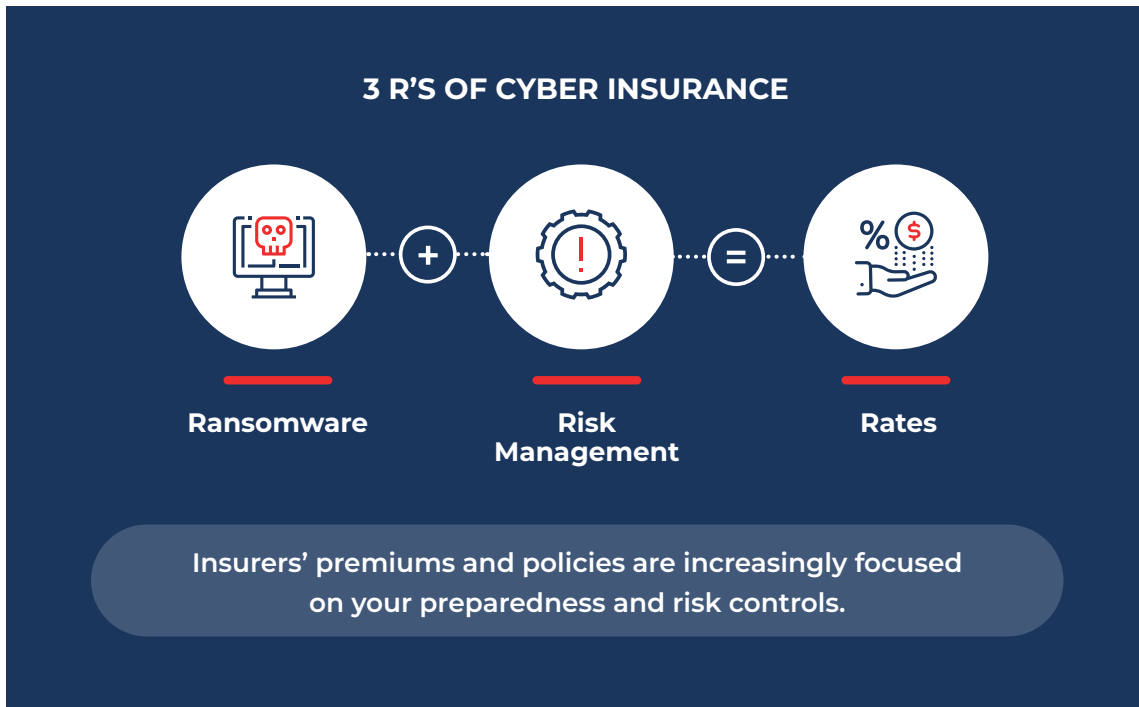


64%

of organizations lack sufficient security measures to prevent a data breach

Your risk profile is the primary variable dictating your policy and renewal outcomes. Insurers are now putting the onus on organizations to better mitigate their risk exposure¹⁴. Organizations perceived to have weak cyber security hygiene are increasingly offered higher premiums, coverage restrictions, or **no coverage at all**.

¹⁴ Q2/Q3 2021 State of the Market Report; [Amwins](#)



Even when a policy is signed, negligence or **failure to maintain adequate security standards** can result in claim denial. This occurred in the case of Cottage Health, whose 2014 data breach was deemed a failure to follow “minimum required practices”, and whose claims were subsequently denied when they were found in violation of HIPAA¹⁵.

With insurers becoming more stringent, what can you do to prevent a cyber insurance claim denial?

Here are five ways to minimize your organization's cyber risk exposure and ensure you've maintained adequate security standards.



¹⁵ Clueless Clause: Insurer Cites Lax Security in Challenge to Cottage Health Claim; [The Security Ledger](#)



5 WAYS TO MINIMIZE YOUR CYBER RISK EXPOSURE AND ENSURE A SUCCESSFUL CLAIM

1

Ensure endpoint protection with a robust EDR solution

One of the most common ways for ransomware to infect your network is through your endpoints—mobile devices, tablets, and laptops connected to corporate networks are all vulnerable points of entry. Most companies rely on legacy defense systems such as antivirus software that simply can't keep up with modern malware, and by themselves, provide poor protection.

For adequate protection, you need a robust endpoint detection and response (EDR) solution that reacts at machine speed to effectively protect your endpoints from malware, such as human-operated ransomware attacks and “double-extortion” attacks that begin with compromised credentials.

Digital Hands' CyGuard® EDR powered by Sentinel One delivers superior threat detection and response with AI-based protection and autonomous response at machine speed.

2

Implement intelligent email filtering tools to catch "phishes"

Email phishing is one of the most common tactics for ransomware to get into your organization's network system. Additionally, the mass use of cloud collaboration tools due to the COVID-19 pandemic has created an increase in unprotected entry points into organizations.

While platforms such as Microsoft Office Suite and Google Workspace include basic email security capabilities, they still miss many advanced attacks. To stay protected, you must implement an intelligent email filtering system that identifies and blocks phishing and ransomware infections before ever reaching your user's inbox instead of retroactively "pulling them out" like legacy defense systems such as Security Email Gateways (SEGs).

Digital Hands' CyGuard Cloud Collaboration & Email Security uses machine learning to learn your company's communication patterns to build custom threat profiles and detect any unusual email/login behavior.

3

Implement and maintain a lifecycle vulnerability management program

As your organization's digital ecosystem expands, it becomes harder to see weaknesses in your network. Vulnerabilities such as unpatched systems, open ports, misconfigured software, and other gaps in your network and endpoints are common points of entry for ransomware.

You need tools that can proactively identify your exposures so you can quickly pinpoint areas of vulnerability and prioritize remediation. Investing in a proper Vulnerability Management Solution ensures that critical vulnerabilities are detected and dealt with rapidly and efficiently.

Digital Hands' Vulnerability Management solution uses advanced threat intelligence to identify vulnerabilities that pose an immediate risk to your company—allowing you to prioritize what needs to be fixed now and what can wait until later.

4

Have a clear security policy

With human error being the cause of 95% of cybersecurity breaches, it's critical for you to have a clear security policy¹⁶. A clear policy outlines organizational rules and enforcement for acceptable IT infrastructure and network use, which sets a high security standard and shows insurers that you've done your due diligence.

This includes strong password protocols, multifactor authentication, privileged access management, and appropriate email usage. Security awareness training for your employees must be conducted regularly throughout the year to ensure your cyber hygiene practices are up to date.

However, even security protocols that fit compliance are no guarantee for protection. For the best results, it's important to work with experts who have the right skills and experience to help you improve your overall cybersecurity posture.

5

Actively manage your cybersecurity protocols with an MSSP like Digital Hands

Effectively mitigating your risks and cyber exposure requires the combined efforts of several individuals across various disciplines in your organization, which is beyond the capabilities of most in-house IT teams. Not only can you avoid cyber insurance claim denial by working with us, but we can in fact **help you get lower insurance rates** by implementing the right security solutions at your organization.

We can also assist with meticulous documentation that satisfies insurer requirements when negotiating a policy or proving due diligence to an insurer after an attack.

¹⁶ IBM Security Services 2014 Cyber Security Intelligence Index; [IBM](#)

STAY PROTECTED & ENSURE PAYOUT WITH DIGITAL HANDS

The impact of ransomware on cyber insurance is not just expensive; it's devastating. In a rapidly evolving threat environment, achieving compliance alone is not enough; it doesn't guarantee protection from ransomware, nor can it ensure a smooth process when submitting a claim. To cover all your bases, it's critical to take a proactive, holistic approach to cybersecurity.

As a new kind of MSSP, Digital Hands is how you can get ahead of cyber threats—by getting to your exposures before the bad guys do. Our unique “See more, Flex more, Do more” approach proactively keeps you steps ahead of ransomware, and provides a clear path for cyber insurance coverage.

The Digital Hands Security Operations Center (SOC) provides coverage when you need it most with the resources to monitor, analyze, and defend your network against any kind of cyber attack.

Digital Hands operates two state-of-the-art 24/7/365 SOC's in Tampa, Florida, and San Antonio, Texas. We do not offshore any of their functions. Our SOC's support our experienced team of cybersecurity professionals who partner with you to create a natural extension to your own IT or security team.

Learn how you can quickly establish a strong security posture and maximize your cyber insurance coverage with our [New Anti-Ransomware Security bundles](#).





ABOUT DIGITAL HANDS

As a new kind of MSSP, Digital Hands is how you can get ahead of cyber threats in a world where compliance alone is no guarantee of protection.

To be truly protected, you must get to your exposures before the bad guys do. You need a "See More, Flex More, Do More" approach that ensures that you're always steps ahead of the latest threats in cybersecurity, safeguarding your organization around the clock, anywhere in the world.

Only Digital Hands brings you this approach. It's why organizations with sensitive data—hospitals, financial institutions, law firms, and government agencies—continue to give Digital Hands an industry-leading CSAT of 98% year after year.

To learn more, visit www.digitalhands.com or [contact us](#).





www.digitalhands.com

(855) 511-5114

4211 West Boy Scout Boulevard Suite, 700 Tampa, Florida 33607

sales@digitalhands.com

2022 © DIGITAL HANDS