TOKIO MARINE HCC

Cyber Liability Insurance

CLAIMS EXAMPLES

Our insureds say it best: "Trusted, responsive, and there when it matters most."

Claims examples are a great way to bring cyber coverage to life, showing how policies respond when it really matters. They help clients understand risks in a relatable way and see the true value of having the right protection in place.
Here are some examples:

01. RANSOMWARE - CYBER EXTORTION

Insured discovered BlackCat ransomware on multiple servers and workstations. Systems were encrypted and insured had no viable backups. Systems contained PII (personal identifiable information), bank information, employee information, and proprietary information bidding software. Immediately upon notice, Tokio Marine HCC (TMHCC) retained counsel and a forensic vendor to assist with the incident. TMHCC then set up a scoping call to ensure the incident was handled as soon as possible. Forensic investigation determined the threat actor gained entry via vulnerability in Microsoft Exchange Server. The ransom demand was originally $1,800,000 but after negotiations with the threat actor, a ransom payment was made in the amount of $300,000. Counsel determined that the Insured had notification obligations and individual notifications were sent out due to potentially exfiltrated data.

There were no escalations by the notified individuals and some enrolled in credit monitoring. Total loss incurred under Breach Event Costs, Cyber Extortion, System Failure Coverages: $506,000. Of that amount, $324,000 was paid under the Cyber Extortion coverage agreement, $86,000 under the Data Recovery coverage agreement, $74,000 was paid under the Privacy Breach coverage agreement, and $18,000 was paid under the Business Interruption coverage agreement.

02. RANSOMWARE – CYBER EXTORTION

The threat actor demanded a $7,000 ransom, but the insured declined to pay—thanks to available backups.

The insured organization discovered Faust ransomware had infiltrated both its email server and the server powering its enterprise resource planning (ERP) system—an essential tool for its manufacturing operations. Both servers were encrypted, halting critical business functions.

Upon being notified, TMHCC immediately activated its Cyber Incident Management team, retaining legal counsel and a forensic investigation firm. A scoping call was promptly arranged to coordinate containment, assess damage, and guide the recovery process.

The forensic investigation revealed that the attacker gained access via a Remote Desktop Protocol (RDP) connection. Fortunately, no evidence of data exfiltration or access to personal information was found. As such, legal counsel confirmed that no regulatory notifications were required. The threat actor demanded a $7,000 ransom, but the insured declined to pay—thanks to available backups. Although the backups were four months old, they enabled full system restoration without engaging the attacker.

Despite avoiding the ransom payment, the insured incurred $125,000 in covered losses, including costs related to:

- **Forensic investigation**
- **Legal counsel**
- **Data restoration from aged backups**
- **System reconfiguration and containment efforts**

This case demonstrates the critical value of cyber insurance—not just for financial recovery, but for expert coordination, compliance guidance, and operational continuity following a disruptive cyber event. Even with some resilience in place, navigating recovery from ransomware without experienced partners would have been far more costly and complex.

03. RANSOMWARE – CYBER EXTORTION

Over a weekend, the insured organization detected a ransomware attack and immediately contacted the Tokio Marine HCC (TMHCC) Cyber Incident Hotline. Within moments, TMHCC's Cyber Incident Management team activated a coordinated response, retaining breach counsel and a leading forensic investigation firm to take swift action.

A scoping call was arranged without delay, enabling a prompt and effective incident response. The ransomware had fully encrypted servers and workstations at the main office, as well as one secondary site's server and backups. However, thanks to the insured's robust cyber preparedness including viable, segmented cloud backups, the organization was able to restore critical systems without paying a ransom.

The forensic team's investigation revealed that the likely method of compromise was a brute force attack on the Fortigate VPN. Legal counsel concluded that, due to strong monitoring and containment, there was no indication of data access or exfiltration, and therefore no notification obligations under data breach laws.

This case underscores the critical advantage of pairing cyber insurance with proactive cyber security controls. The insured avoided prolonged downtime, regulatory exposure, and ransom payment incurring only the following covered breach event expenses:

- **Forensic Investigation: $27,000**
- **Legal Counsel: $5,000**

Through rapid coordination, expert support, and strong internal resilience, the insured minimized both operational disruption and financial impact.

This case underscores the critical advantage of pairing cyber insurance with proactive cyber security controls.

04. RANSOMWARE – CYBER EXTORTION

On November 20, 2024, the insured discovered a ransomware attack and immediately contacted the TMHCC Cyber Incident Hotline. Within moments, TMHCC's Cyber Incident Management team mobilized a response—retaining legal counsel and a forensic investigation firm to assess and contain the breach. A scoping call was quickly arranged to align the recovery strategy.

The attackers issued an initial ransom demand of $2,000,000, prompting the insured to explore recovery alternatives. Unfortunately, only limited backup data was available, restricting the insured's ability to fully restore operations without the decryptor. As the incident unfolded during the Thanksgiving holiday, time was of the essence. The cyber extortionists imposed a steep deadline: failure to pay the ransom before the holiday weekend concluded would result in a $600,000 increase in the ransom demand.

Thanks to the real-time availability and coordination of TMHCC's Cyber Incident Management and Claims teams, internal approval was obtained on Thanksgiving Day for a $1,020,000 ransom payment. This allowed the insured to secure the decryption tool and restore critical operations by the following Monday—avoiding both additional extortion costs and prolonged business interruption.

To date, the following covered expenses have been paid under the policy:

- **Cyber Extortion Payment: $1,024,000**
- **Breach Event Costs (Forensics & Consultants): $64,900**

This case powerfully illustrates the value of cyber insurance—not only for significant financial protection, but for immediate crisis response when timing is critical. TMHCC's around-the-clock support and claims agility enabled the insured to avoid deeper operational and financial fallout during a high-pressure holiday incident.

05. RANSOMWARE – CYBER EXTORTION

Upon discovering a ransomware attack, the insured immediately contacted the Tokio Marine HCC (TMHCC) Cyber Incident Hotline. The Cyber Incident Management team promptly responded and retained breach counsel and a forensic investigation firm to take charge of the incident. A scoping call was conducted without delay to coordinate containment and recovery efforts.

The attackers issued an initial ransom demand of $1,160,000. During the forensic investigation, it was discovered that the threat actor had used a file-sharing site to steal and host the insured's data and had inadvertently left access open. In a strategic move, the forensic vendor leveraged the threat actor's own credentials to copy and delete the insured's data from the site, significantly reducing the risk of exposure and removing the data from circulation.

There was continued negotiations with the attacker, ultimately securing a reduced ransom settlement of $316,500—a substantial reduction from the original demand.

While the data was successfully recovered and removed, the insured still required the decryptor tool to fully restore operations. There was continued negotiations with the attacker, ultimately securing a reduced ransom settlement of $316,500—a substantial reduction from the original demand. Counsel later confirmed there were no notification obligations, as no sensitive personal information had been accessed or exfiltrated.

To date, the insured has incurred the following covered expenses:

- **Breach Event Costs: $29,000 (for forensic investigation and privacy counsel)**
- **Cyber Extortion: $340,000 (ransom payment and related fees)**
- **System Failure Coverage: $20,000 (data restoration services)**

This case shows the multifaceted value of cyber insurance: not only in offsetting financial loss, but in orchestrating a highly strategic and effective response, one that prevented data exposure, significantly reduced the extortion payment, and helped the insured swiftly restore operations with minimal disruption.

06. RANSOMWARE – CYBER EXTORTION AND BUSINESS INTERRUPTION

Insured's internet and phone service provider, their "outsourced IT service provider", suffered an outage due to a ransomware attack. Insured's phone system was down for 38 days which led to slightly lower sales and they experienced a business interruption loss due to the outage. TMHCC retained a forensic accountant to help determine the Insured's business interruption loss of $12,000. Total loss incurred under System Failure Coverage: $18,000.

Of that amount, Business Income loss paid $12,500 under the cyber insurance policy and Forensic Accounting Fees paid $5,500.

Insured's phone system was down for 38 days which led to slightly lower sales and they experienced a business interruption loss due to the outage.

07. BUSINESS EMAIL COMPROMISE – WIRE TRANSFER FRAUD

The insured organization suffered a significant financial loss after receiving an email that appeared to be from a trusted client, requesting the transfer of $1.9 million. Believing the request to be legitimate, the insured wired the funds—only to later discover the request had been fraudulent. Despite multiple attempts, the insured was unable to recover the funds through its banking institution.

Several months later, the insured contacted Tokio Marine HCC (TMHCC)'s Cyber & Professional Lines Group for assistance. The Cyber Claims team immediately provided step-by-step guidance and leveraged both law enforcement and banking contacts to help pursue fund recovery.

> As a result of this coordinated effort, $925,000 of the misdirected funds were successfully recovered.

As a result of this coordinated effort, $925,000 of the misdirected funds were successfully recovered. In addition, the insured's cyber policy included $250,000 in phishing fraud coverage, which was paid in full—significantly reducing the financial impact of the loss.

This incident is a powerful reminder of the value of cyber insurance—not only for financial reimbursement, but for access to experienced professionals who advocate for policyholders long after an incident occurs.

"I cannot thank you enough for doing that and helping us get back some of the dollars lost. It's nice to be reminded that good people are out there in the business world who are still willing to lend a hand even when it doesn't necessarily benefit them directly."— Insured

Even in the face of substantial loss, the insured was able to regain control of the situation with the support of a carrier committed to meaningful results and service.

08. BUSINESS EMAIL COMPROMISE – WIRE TRANSFER FRAUD

The insured received what appeared to be a routine email from a trusted vendor, requesting payment via ACH for an outstanding invoice totaling $90,000. The request included payment instructions on the vendor's official letterhead, adding to its credibility. Unbeknownst to the insured, the email was spoofed and the payment details were fraudulent.

The transfer was made in good faith, but the fraud was only discovered when the legitimate vendor followed up, inquiring about the missing funds.

Upon being notified, TMHCC's Cyber Claims team immediately provided guidance, including detailed steps for pursuing potential recovery through the insured's banking institution. Acting quickly and following the expert advice provided, the insured was able to successfully recover the full amount of the transfer.

While no insurance payout was required in this instance, the event demonstrates a critical value of cyber insurance: access to expert support and resources when faced with unexpected cyber threats. The swift response and actionable guidance enabled the insured to resolve the issue efficiently and avoid a significant financial loss.

Even when financial losses are recovered, the ability to lean on knowledgeable partners during a crisis is a powerful benefit demonstrating that cyber insurance is not just a policy, but provides a trusted partner in moments of uncertainty.

9. BUSINESS EMAIL COMPROMISE – WIRE TRANSFER FRAUD

A hotel management firm, responsible for handling lease payments on behalf of its client, received what appeared to be a legitimate email request to transfer $450,000 for a lease payment. Unfortunately, the email was a convincing spoof, part of a sophisticated business email compromise (BEC) scheme, and the requested funds were unknowingly sent to a fraudulent account.

By the time the discrepancy was discovered, the funds could not be recovered. Fortunately, the Insured had a cyber insurance policy with Tokio Marine HCC (TMHCC), which included a $250,000 cyber crime sublimit. While the financial loss from the incident was significant, the cyber coverage helped offset over half of the loss. TMHCC responded promptly and paid the full $250,000 sublimit, alleviating the financial burden on the insured and closing the claim.

This incident highlights the unpredictable nature of cyber threats and the essential role cyber insurance plays in safeguarding organizations from financial fallout. In an increasingly digital world where threat actors are constantly evolving their tactics, cyber coverage serves as a critical safety net when prevention alone isn't enough.

10. PRIVACY AND DATA BREACH

The insured's information, as well as their clients' information stored on the platform was compromised.

Insured was contacted by Github, a social and collaborative platform for developers, that their personal access token (PAT) was compromised. The insured's information, as well as their clients' information stored on the platform was compromised. TMHCC allowed the Insured to use their preferred counsel, subject to a rate cap. The Insured already retained a forensic vendor and obtained a SOW (scope of work) which was reviewed by TMHCC and ultimately approved for use.

The Insured wanted to perform data mining, as there was some PII (personal identifiable information) found in the impacted data, to determine if there were any notification obligations but there were not. Total Costs for Forensic Investigation was $55,000, Data Mining was $7,000; Total paid under the cyber insurance policy was $62,000.

11. PRIVACY AND DATA BREACH

Plaintiffs filed a putative class action lawsuit alleging the insured breached confidentiality and unlawfully disclosed plaintiffs PHI/PII to Facebook, violating CMIA and CIPA. The complaint alleges the insured's website contained Pixel's tracking the pages visited, the buttons clicked, and specific patient info entered into fillable forms. Forensics determined that Pixel was present on every page of the insured's website but was not present on the patient portal.

Further, none of the pages obtained patient PHI and found no evidence this was being transmitted by Pixel to Facebook. However, Pixel was sending click info to Meta, along with IP addresses belonging to the website visitors, the web browser being used, and the type of operating system being used. If a user was logged into Facebook when visiting the insured's website, the users Facebook profile name was also sent back to Facebook. Plaintiffs' initial demand was $15,000,000 which was negotiated down to a $1,750,000 settlement. TMHCC retained defense counsel to assist in resolving the matter without proceeding with litigation. One member opted out of settlement and filed a complaint – their initial demand was $20,000 which was negotiated and settled for $5,000.

The total loss to date under Security and Privacy Liability Coverage, $1,755,000 (indemnity), $205,600 (legal expenses), $85,400 on reserves.

12. PRIVACY AND DATA BREACH

Throughout the matter, Tokio Marine HCC provided legal defense coverage, incurring and covering $16,000 in legal expenses to protect the insured's interests.

A former employee filed a putative class action lawsuit against the insured, alleging that during her employment she was required to use her fingerprint to clock in and out of work without having provided proper consent. The complaint claimed that neither the plaintiff nor other employees were informed of the collection, use, or retention policies regarding their biometric information, in violation of biometric privacy laws. Although the insured did not directly collect or store any biometric data—the process was managed by their staffing company—they were nonetheless named in the lawsuit. The staffing company had, in fact, secured proper consent and was able to produce signed authorization forms, ultimately demonstrating compliance. As a result, plaintiff's counsel voluntarily dismissed the case.

Throughout the matter, Tokio Marine HCC (TMHCC) provided legal defense coverage, incurring and covering $16,000 in legal expenses to protect the insured's interests.

This claim illustrates the importance of cyber and privacy liability coverage in today's regulatory environment. Even when an organization follows best practices or outsources data collection to a third party, it can still face costly legal allegations. Having cyber insurance in place ensures organizations are supported with both financial protection and legal expertise when unexpected privacy-related claims arise.

13. LICENSE AGREEMENT VIOLATION

DEA Lookup.com, a third-party software provider, alleged that the Insured violated the End User License Agreement (EULA) for its "License Lookup" software, a tool used to verify DEA registrations and prescribing authority. The third-party claimed the Insured had paid for 8 licenses however it allowed at least 55 employees to access the software, and improperly installed the software on a Citrix server, granting access to up to 277 employees. The third-party initially demanded $1,750,000 in damages and a 10-year licensing agreement at $45,000 annually. TMHCC retained defense counsel to assist in resolving the matter without proceeding with litigation.

Following extensive negotiations, the parties reached a pre-litigation settlement agreement of $435,000. Additionally, the Insured entered a three-year licensing agreement for 12 users at $69,300, paid directly by the Insured.

The settlement included mutual releases, confidentiality provisions, and non-disparagement clauses, with the Insured confirming compliance with the EULA and removal of unauthorized software copies. Total costs after $50,000 deductible was $416,010:

- **Defense costs: $12,410**
- **Settlement: $403,600**

Following extensive negotiations, the parties reached a pre-litigation settlement agreement of $435,000.