



Insurance & Federal Claims Services

Cyber and network security
insurance claims

June 2022



EY

Building a better
working world

Overview

The Insurance & Federal Claims Services practice of Ernst & Young LLP helps companies to accurately measure, document and prepare complex insurance claims, including those caused by cyber and network security issues. We help clients anticipate claims process challenges to reduce delays in recovery, expedite the process of documenting potential claims and assist with fully identifying all recoverable costs, which speeds the recovery of cash associated with the loss.

The complexities of the insurance policies regarding instances of ransomware and cyber attacks are unique and challenging. These insurance contracts often include several policies that address business interruption, property damage, software kidnapping, and crime and fidelity. In addition, with multiple claims there could be numerous insurers and several insurance adjusters working around one related incident. We assist companies in properly navigating the complexity of these cyber and network security claims and accurately determining the costs that can be recovered.

Ransomware and cyber attack costs covered by insurance

Adequate security standards to help prevent and even mitigate any potential damages caused by ransomware and cyberattacks are mandates for most insurance policies. Some policies may exclude recoverable costs depending on the insured's business practices, the occurrence of the cyberattack and the policy overall. Cyber insurance policies vary, and some may provide coverage for:

- ▶ Lost revenue from a cyber attack that negates day-to-day operations and services.
- ▶ Regulatory fines for data breaches.
- ▶ Legal defense fees incurred from any data breaches.
- ▶ Costs related to hiring cybersecurity professionals to determine and repair any security flaws in current systems.
- ▶ Credit monitoring service costs for parties impacted by a data breach or cyber attack.
- ▶ Ransoms paid to recover systems.

Sample experience

The Insurance & Federal Claims Services practice provided claims preparation assistance for a physical damage and product recall loss at a Fortune 500 computer manufacturer that was maliciously attacked by a hacker. By collaborating with the company, our team assisted with the quantification of loss and resolution of the claim within three months of the event.

Our team assisted one of the world's largest food manufacturers with the preparation of a business interruption, extra expense and property damage claim as a result of a global ransomware campaign, which severed communication and operations from their global network. We worked with multiple points of contact around the world to fully understand the global impact and present the insurance claim for resolution.

Our team helped a global services firm with its preparation of an eight-figure loss due to a cyber attack by overseas hackers. We worked in seamless collaboration with the EY Cybersecurity team to map losses to potential opportunities for recovery under the company's policy.

Our team assisted a hospital system with its response and recovery following a ransomware attack. The EY Cybersecurity team successfully assisted the client in their ransom attack response to help mitigate the negative impacts of the attack. After the ransomware was cleared from the network, our team assisted the client in preparing a business interruption, property damage and extra expense claim that spanned multiple policies. We assisted in quantifying the damage to the network, including replacing imaging servers, computers and network equipment as well as the business interruption impact of this breach.



Dedicated team of multidisciplinary professionals

We provide a deep bench of in-house resources to comprehensively address a full range of cyber insurance issues, from policy planning to claims. Our team includes:

- ▶ Former adjusters, forensics accountants and claims managers from major international insurance companies and their consultants
- ▶ Dedicated industry professionals who bring relative industry insight to complex risk-and-loss scenarios
- ▶ More than 60 forensic technology centers worldwide to help companies from all sectors address complex strategy, policy and technical challenges in high-pressure and high-visibility situations
- ▶ Proven industry professionals who have extensive experience in more than 30 industries, including former insurance adjusters and claims auditors

“

In recent times, the frequency of ransomware attacks and large data breaches are causing companies and insurers to face more expensive business interruptions and other claims.



BJ Nichols
Insurance & Federal Claims Services Leader

Highlights and qualifications

Global capabilities: we have assisted with claims on six continents. Our global team of proven professionals is staffed to respond immediately to challenges wherever they occur.

Deep technical knowledge: we offer integrated, focused industry knowledge that helps organizations identify exactly what happened technologically and determine how that may fit into the company's policies.

Confidentiality: we understand the need for and importance of confidentiality. All claims necessitate a degree of secrecy, and our teams fully understand that data breach losses can damage reputations and warrant extra caution and discretion.

Scalable approach: our skilled professionals have the flexibility to handle claims of all sizes and complexities.

Objectivity and fresh perspective: we are a trusted and objective advisor in the claims process. We understand organizations' businesses, educate internal and external stakeholders and leverage knowledge and technology to improve the efficiency within the claims management process.

High-touch, effective service: our team provides objective analyses and alerts clients of current trends, new ideas and differing processes to potentially enhance the strategy of their overall risk management.

Fee-neutral: while fees for services provided by our team may be covered within the terms of a client's policy, our fees are based on the quality of our services and are not contingent on the outcome of settlement.

What can cause a cyber or network security insurance claim?

The answer is continuing to evolve, but it is not universal. Most cyber insurance claims are the result of employee mistakes and human error. Equally, most external cyber attacks, such as distributed denial of service attacks, phishing and ransomware/malware campaigns, are more costly to those affected. Some scenarios that include cyber crime and/or triggers for a cyber insurance claim may include:

- ▶ Extortion payments made by the company in the event of a ransomware attack.
- ▶ Funds transfer fraud attacks and business email compromises (BEC); a company is tricked into making a payment into an attacker-controlled account.
- ▶ Distributed Denial of Service attacks where a company's servers crash due to the high volume of traffic directed to it by cyber criminals.
- ▶ Email hacks or other unauthorized actions (phishing, shoulder surfing, etc.).
- ▶ Juice jacking: compromise of devices like phones and computers that use similar data cables (charging/data transfer/USB) to install malware on the device.
- ▶ Document manipulation or destruction.
- ▶ Access to sensitive business data being shared unlawfully by a company employee.
- ▶ Sophisticated equipment breached, impacting efficiency and resulting in decreased or lost production.
- ▶ The high cost (financial and reputational) of communicating to customers that their sensitive information has been exposed.

Our Insurance & Federal Claims Services team can help clients recover from cyber and network security incidents, and expedite recovery of costs associated with possible claims.

Insurance & Federal Claims Services Team

Forensic & Integrity Services

Ernst & Young LLP

Bradley (BJ) Nichols

Insurance & Federal Claims Services Leader
bradley.nichols@ey.com

Jill E. Powell

Principal
jill.powell@ey.com

Jeff Phillips

Managing Director
jeffrey.phillips@ey.com

Allen Melton

Partner
allen.melton@ey.com

Doug Farrow

Managing Director
doug.farrow@ey.com

Brad McCloskey

Managing Director
brad.mccloskey@ey.com

Robert M. Reeves

Partner
robert.reeves@ey.com

Nigel Henley

Managing Director
nigel.henley@ey.com

Allen Shank

Senior Manager
allen.shank@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2022 Ernst & Young LLP.
All Rights Reserved.

SCORE no. 16142-221US

2203-4003058
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/forensics/insurancefederalclaims