



CORVUS GUIDE TO:

Your Coverage

Risk Mitigation, Claim Notice & Incident Response

You're flying with Corvus! From all of us at Team Corvus, thank you very much for choosing us for your Smart Tech E&O™ policy. Here you'll find an overview of the features of your policy and how we'll handle claims and incident response. We hope this guide helps you feel comfortable and familiar with the policy and procedures. Should you have any questions about what to do in the event of a claim or incident, don't hesitate to reach out to me directly.

Mike Karbassi

Head of Cyber Underwriting

mkarbassi@corvusinsurance.com

In this guide you'll find:

.....
Page 2: Coverage Overview
.....

Page 3: Risk Mitigation Overview
.....

Page 4: Claim Notice and Incident Response Procedure
.....

Page 6: How to access your Risk Management Portal
.....



Coverage Overview



Corvus's Smart Tech E&O™ policies offer broad first-party and third-party coverages, as well as options for additional coverage enhancements. This is summary information only. Please review your policy for full detail on your coverage.

THIRD-PARTY COVERAGES

Network Security and Privacy Claims: Claims against you because of a network security or privacy breach. This may arise from a denial of service attack, malicious code, a stolen laptop, or any type of data breach.

Regulatory Investigations, Fines and Penalties: Civil fines and penalties imposed by a governmental agency as a result of a breach of privacy regulations.

Media Liability Claims: Claims against you arising from the release or display of your media material. This includes claims alleging copyright infringement, slander, libel, defamation, and other media perils.

PCI DSS Assessment Expenses: Forensic investigation costs, fines, penalties and assessments you are legally responsible for as a result of actual or alleged non-compliance with Payment Card Industry Data Security Standards.

Breach Management Expenses: Breach response costs for which you have contractually indemnified a third party for a security or privacy breach.

Technology and Professional Services Liability: Coverage for damages and claims expenses arising from both tech-based services and other professional services offered by the insured. Claims stemming from the failure in tech products are also covered.

Software Copyright Infringement: Coverage for actual or alleged copyright infringement.

ADDITIONAL COVERAGE ENHANCEMENTS ARE AVAILABLE:

- Bricking Coverage
- Forensic Accounting Coverage
- Criminal Reward Expenses
- Invoice Manipulation
- Bodily Injury
- Preventative Shutdown

FIRST-PARTY COVERAGES

Business Interruption: Business income loss and extra expenses you incur during a computer network outage.

Contingent Business Interruption: Business income loss and extra expenses you incur during a network outage at your outsourced service provider.

Digital Asset Destruction, Data Retrieval and System Restoration: Digital asset loss and related expenses you incur as a result of a security breach, privacy breach, or administrative error.

System Failure Coverage: Business income loss, extra expenses, and digital asset loss you incur during an unintentional or unplanned outage.

Social Engineering & Cyber Crime Coverage: Financial fraud, phishing attack loss, and telecommunications fraud loss you sustain as a result of a social engineering event or impersonation attempt.

Reputational Loss Coverage: Business income loss you may suffer related to a media report arising from a privacy breach, cyber extortion threat, or phishing attack.

Cyber Extortion and Ransomware Coverage: Your expenses or payments to respond to a cyber extortion demand or ransomware attack.

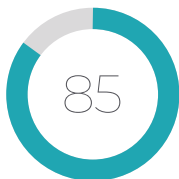
Breach Response and Remediation Expenses: Your expenses to respond to a data breach incident including legal services, forensics investigation, notification, credit monitoring and public relations.

Court Attendance Costs: Expenses you incur to attend court, adjudication, mediation or other hearing in connection with a covered claim.

Preventative Resources: Risk Mitigation



No broker wants their client to experience a cyber attack.
With Corvus, you and your clients have access to preventative
resources that can help mitigate risk.



DYNAMIC LOSS PREVENTION

Scans your IT exposure and provides prioritized recommendations throughout the policy period so that corrective action can be taken before vulnerabilities are exploited. Go to [CorvusInsurance.com](https://www.corvusinsurance.com) to learn more about how to use this resource.



SMART CYBER RISK MANAGEMENT PORTAL

Provides comprehensive resources and risk management tools aimed at helping your client and their employees understand and prevent risk in your daily operations. See the last page of this document for more information.



\$1,000,000 COVERAGE IN PRE-CLAIM SUPPORT SERVICES

For a potential loss or claim, and a free consultation with a breach attorney. Contact us to learn more.

Claim Notice And Incident Response



In the event of a privacy breach or other claim, you have a few options for a first step. **You may:**

- Email:
teoclaims@corvusinsurance.com
- Call the Corvus 24/7 Breach Response Hotline: **(844) 916-0087**
- Contact a Breach Coach via the Smart Cyber Risk Management Portal



CRUM & FORSTER®

A FAIRFAX COMPANY

In handling claims, Corvus works closely with our risk-taking partner Crum & Forster. C&F is recognized for providing superior service based on responsiveness, a collaborative approach and cumulative knowledge. The company has more than 500 claim professionals nationwide, with specialized expertise in Cyber and Technology E&O.

Every situation is unique. Upon receiving your email or call, the Claims Team will help you determine the appropriate next steps. They will first determine:

- Your computer forensics investigation needs
- Breach notifications requirements
- Potential for regulatory fines and/or legal action

Based on your needs, the Claims Team will contact partners who specialize in different aspects of response procedure.

Our partners include expert **privacy attorneys** who can help to determine legal applicability of actions to respond to reporting requirements and maintain privilege.



MULLEN
COUGHLIN



WILSON ELSE
WILSON ELSE MOSKOWITZ EDELMAN & DICKER LLP

troutman
sanders



Claim Notice And Incident Response



The Team may also may engage partners to conduct computer forensics to determine the existence, cause and scope of the breach.



Next, we'll help determine if customer notification and/or credit monitoring is required, and engage with partners who can assist you in setting up a call center.



We'll also assist with breach remediation, which may include coordinating an information security gap analysis with one of our partners.



Should the situation require, the team will also help you to hire a PR or crisis communication firm.



Finally the Claims Team will discuss your next steps to recover from the incident and restore customer trust. No matter what the situation requires, the Corvus and the Claims Team will be with you every step of the way.

More detailed information on Incident Response can be found in the **Smart Cyber Risk Management Portal** (accessible via the CrowBar - see last page of this document).

Claims at C&F Meet the Team



C&F is recognized for providing superior service based on responsiveness, collaborative approach and cumulative expertise.

Kristine D'Amato, Director, joined the Executive Risk Claims Department in April 2017. Kristine is an attorney with over 15 years of experience in the insurance industry. Prior to joining Crum & Forster, Kristine oversaw a team that handled a wide variety of complex D&O, EPL and E&O claims for Liberty International Underwriters as Assistant Vice President, and handled claims across those lines for Liberty since 2011. Prior to that, Kristine was a Claims Consultant in the D&O group at the Hartford, and began her career in private practice. Kristine received her J.D. from Fordham University School of Law in New York, and her B.A. from S.U.N.Y Binghamton.

John R. Cascarano, Senior Specialist, joined the Executive Risk Claims Department in January 2019, and has been with Crum & Forster since 2017, handling complex construction defect and environmental claims. Prior to joining Crum & Forster, John was an attorney who specialized in commercial litigation, government, and municipal practice, serving as an Assistant Prosecutor in the Office of the Hudson County Prosecutor's Office, as well as counsel to the New Jersey State Legislature and Governor of New Jersey. John received his J.D. from Seton Hall University School of Law in New Jersey, and his B.A. from Montclair State University.

Morissa Falk-Freedman, Executive Specialist, joined the Executive Risk Claims Department in October 2017. Morissa is an attorney with over 11 years of experience litigating and working in the insurance industry. Prior to joining Crum & Forster, Morissa handled a wide variety of complex E&O and Cyber claims for Liberty International Underwriters. Prior to that, Morissa litigated complex antitrust and products liability cases. Morissa received her J.D. from Brooklyn Law School, and her B.A. from Haverford College.

Anne Marie Foersch, Executive Specialist, joined the Executive Risk Claims Department in June 2011. She has been with C&F since 2001 and brings over 20 years claim experience to her position. Anne holds a B.S. degree from Rutgers University in New Brunswick, New Jersey and the CPCU, AIC and ASLI Designations from the Institutes.

Shimon Getler, Executive Specialist, joined the Executive Risk Claims Department in September 2018. Shimon is an attorney with 18 years of experience in the insurance and financial services industries. Prior to joining Crum & Forster, Shimon was an Assistant Vice President & Claims Counsel at Sompo International for more than nine years, handling mid-range and high level exposure claims in the E&O, Financial Institutions and D&O space. Prior to that Shimon was an Assistant General Counsel at UBS Financial Services, and began his career in private practice. Shimon received his J.D., cum laude, from New York Law School, and his B.A., magna cum laude, from S.U.N.Y. Buffalo.

About the Smart Cyber Risk Management Portal



With Corvus, you and your clients have access to preventative resources that can help mitigate risk.

The Smart Cyber Insurance Risk Management Portal is accessible to all Corvus brokers and policyholders. It is accessible through the CrowBar™, our insurance platform. The Portal contains:

- Incident roadmap with detailed information about the Incident Response procedures summarized in this document
- Library of articles with important information about cyber risk and security practices
- Courses and quizzes for security training
- Risk management tools including a data breach cost calculator
- Key contacts for security and incident response vendors and experts

The screenshot shows the top navigation bar of the Corvus CrowBar platform. The navigation bar includes the Corvus logo, a 'Home' button, and several menu items: Incident Roadmap, News Center, Learning Center, Security Training, Risk Manager Tools, and Vendors & Experts. On the right side of the navigation bar are search and contact us icons. Below the navigation bar, the title 'Smart Cyber Insurance™ Risk Management Portal' is displayed. Underneath the title, there are four main sections, each with an icon and a brief description: 1. Breach Coach®: Contact a Breach Coach if you suspect a data breach. 2. Breach Roadmap: Learn how you should respond to a data breach. 3. Cyber Tools: Access tools to evaluate your risk and bolster your defense. 4. Learning Center: Extend your knowledge of security, privacy &.

To access the Risk Management Portal:

- Log into CrowBar at crowbar.corvusinsurance.com.
- Click "Resources" in the top navigation
- At the bottom of the bulleted list, find the link for Smart Cyber Risk Management Portal

From there you will automatically be logged into the portal with access to all resources. There is no limit to the number of members of your team who can access the portal.