CHUBB®

Cyber Claims Scenarios

Here are examples of recent claims scenarios to give you a sense for our capabilities:

Unauthorized Access

Industry	Professional Services
Business	Commercial
Claims Difference	Top-Tier Response Coach and Forensic Firm
Description	Our Insured is a professional organization that has an online portal for its members to access data. The organization experienced a security incident and its service representatives noticed that in a number of instances, member registration information was incorrect and that there had been a scrambling of data. A incident response coach and a forensic service firm from our cyber panel were engaged and it was determined that unauthorized access occurred on one of its servers providing external web portal functionality. The forensic firm did not find any evidence that personally identifable information was disclosed during the attack and the data returned from the Insured's database was nonsensitive. Chubb paid approximately $100,000 CAD in 1st party costs associated with this matter.

Ransomware Attacks

Industry	Professional Services
Business	Commercial
Claims Difference	Top-Tier Response Coach and Forensic Firm
Description	A professional services firm experienced a ransomware attack which encrypted several files on its servers. A ransom of approximately $10,000 was initially demanded. We were promptly notifed of the event through our cyber incident response hotline and an incident response coach and a forensic firm that specialized in ransomware were retained from our cyber panel. After consulting with these experts, the Insured decided to pay the ransom. Upon payment of the ransom, the Insured was able to begin the decryption process. Following an investigation by the forensic firm, it was determined that no personally identifable information was compromised as a result of the attack. As a result of the ransomware attack, the Insured incurred losses of approximately $100,000, which was comprised of $15,000 for the incident response coach, $75,000 for the forensic firm and $10,000 for the ransom payment.

CHUBB®

Phishing Emails

Industry	Financial Services
Business	Commercial
Claims Difference	Expert Claims Investigation
Description	Employees of a midsize financial services company fell victim to a mass phishing attack by clicking on a link that enabled the bad actors to obtain system credentials which allowed them to access email accounts. Approximately 100 email accounts were compromised and the bad actors set a forwarding rule that sent new emails to an unauthorized webmail address. Many of the email accounts contained names and social security numbers of the Insured's clients. A cyber incident response coach and a forensics firm that frequently deals with these types of phishing scams were retained from our cyber panel. Utilizing specialized tools to analyze which email accounts were comprised, the forensics firm concluded that several million documents needed to be reviewed to determine the nature and scope of the affected population. Additionally, the bad actors were able to access the Insured's other systems to cause several fraudulent wire transfers to take place. It was eventually determined that 200,000 people needed to be notifed and provided with two years of credit monitoring. Total first party losses were approximately $3.5M, broken down as follows: $2M for the forensics firm, $1M for the incident response coach and $500,000 credit monitoring and call center fees.

Vendor/Supply Chain

Industry	Healthcare
Business	Commercial
Claims Difference	Technical Expertise
Description	A business associate of the Insured fell victim of a ransomware attack that encrypted many of its files. The business associate possessed medical records and personal health information of the Insured's customers and had to retain an incident response coach and forensic firm to remedy the ransomware attack on its system. While our Insured had previously utilized Chubb's pre-incident services to better prepare for a breach, the Insured still needed to consult with its own incident response coach from our cyber panel to determine what reporting obligations it had under HIPAA. The incident repsonse coach eventually determined that there was no exfiltration of personal health information from the business associate's system. As a result of the incident, the Insured incurred $20,000 in first party costs.

Ready to sell Chubb?

Visit our website for more information about Chubb's insurance solutions.