CohnReznick

# Incident response and recovery services

## What we do

### Incident response

Our team of responders works with organizations to manage, recover, and remediate cyber incidents and data breaches. Additionally, we offer resiliency training and simulations to prepare for potential threats, and forensics and cyber litigation support for specialized investigations and legal actions following data breaches.

### Threat detection

Our team deploys tools and techniques to identify active threat actors in your environment. We use the latest digital forensics, data analytics, and investigative tools and techniques.

### Data collection & preservation

We collect evidence across your networks and devices with minimal business disruption and preserve electronic evidence so it will withstand scrutiny in anticipation of future litigation.

### Forensic analysis

Our state-of-the-art digital forensics lab combines the latest forensic tools with vast computing power and data throughput in a secure, dedicated environment.

### System recovery

We can augment your existing IT team with experienced responders to expedite your recovery. Our techniques will help you resume business operations faster while preserving evidence.

### Security remediation

We identify and remediate vulnerabilities in your systems to protect you from future attacks. The team implements Active Directory hardening, cloud migrations, privileged access management deployment, and other measures necessary to strengthen your environment.

### Damage quantification

We help organizations assess the financial impact of a cyber incident. Using operational data and key loss factors, we quantify the economic consequences of an incident. This enables businesses to make informed decisions, support potential litigation, and optimize insurance claims.

### Expert testimony

Our team members hold multiple forensic certifications, have testified as experts in US state and federal courts and regularly provide counsel with clear and useful information.

# Our experience

Our team has vast experience in all types of incidents, including ransomware, business email compromise, network intrusions, wire fraud, and insider data theft.

### Sample experience:

- **Business email compromise:** Worked with a health insurance claims processor to identify a compromised account. Reviewed tenant to ensure no evidence of additional compromises. Conducted data mining to identify list of hundreds of thousands of impacted individuals.
- **Ransomware attacks:** Responded to ransomware attack at a third-party logistics company. Conducted forensic triage, assessed severity of impact and identified scope of ransom negotiation to reduce costs.
- **System recovery:** Responded to ransomware attack at a large real estate development and management group. Assisted with system recovery and rapid overhaul of antiquated systems.
- **Malware analysis:** Assisted office supply company with compromised eCommerce site. Identified and reverse-engineered card capturing malware. Quantified list of potentially compromised cards.
- **Business email compromise:** Worked with healthcare network to identify compromised account leading to $2.4 million in fraudulent wires. Reviewed tenant to ensure there was no evidence of compromised personal health information.
- **Threat hunt:** Conducted a threat hunt at a publicly traded biotech pharmaceutical company. Deployed tools to analyze telemetry and rapidly determine cause of suspicious activity.
- **Forensic analysis:** Assisted staffing company with internal investigation. Identified employees who were diverting business to competitors and sending inflammatory anonymous emails to clients and interested parties.
- **Malware analysis** Responded to a cyber attack on a nonfungible token studio. Identified root cause of cryptojacking and assisted client in recovery.
- **Data breach:** Conducted investigation of internal data breach at a healthcare network. Identified internal employee who made unauthorized copy of protected healthcare information. Identified copied information and provided data set to client for analysis and data mining.
- **Damages calculation:** Assisted owners of restaurant group impacted by a ransomware attack that shut down online sales and orders. Reviewed financial statements before, during, and after the incident to determine lost profits directly attributable to the incident. Provided opinion and supporting analysis to insurance carrier for claims processing.

# Contact


**David Sun**
Partner, Cybersecurity,
Technology Risk and Privacy
703-744-8508
david.sun@cohnreznick.com

**Bhavesh Vadhani**
Partner, Cybersecurity,
Technology Risk and Privacy
703-847-4418
bhavesh.vadhani@cohnreznick.com

**Incident Response Hotline**
833-854-8371
incidents@cohnreznick.com




CohnReznick