Claim Case Study: Business Email Compromise

How Cowbell helped the policyholder recover quickly with minimal loss

This case study provides an overview of the claim's process at Cowbell

Who was the victim?

Industry	Revenue:	Employee count:	Location:	Type of incident:
Construction	$30,000,000	Less than 100	Kansas	Business Email Compromise

What happened?

- The policyholder saw that a bad actor was spoofing their email domain to send fraudulent payment requests internally
- Once the policyholder realized that, it notified Cowbell immediately

The policyholder immediately contacted Cowbell.

How did Cowbell help?

Within one hour of notification, Cowbell's claims team worked with the policyholder to:

1. Acknowledge the receipt of the claim and provide initial advice on recommended next steps;
2. Line up breach counsel and forensic teams for a scoping call;
3. Approve vendor workstreams;
4. Conduct a preliminary coverage review to confirm coverage.

Thanks to Cowbell's assistance, the policyholder was able to recover its environment within days, confirm that any unauthorized access did not trigger legal notification obligations, and most importantly - prevent unauthorized and fraudulent wire transfers.

Business Email Compromise is often used as a means of phishing attacks. According to smallbiztrends.com, **83%** of organizations faced a successful email-based phishing attack in 2021.

Cyber incidents happen. What's important is that you take measures to protect yourself and prepare your organization to respond to potential cyber events.

Cowbell's cyber policies include a wealth of resources to help you stay ahead of today's and tomorrow's threats. Our risk engineering team is available to advise you on cybersecurity measures to implement and how to take advantage of all resources provided.

The Leader in Cyber Insurance for SMEs

Cowbell delivers standalone and individualized cyber insurance to small and medium-sized enterprises. Cowbell's cyber policies include continuous risk assessment, access to risk engineers for advice, cybersecurity awareness training for employees, and more.