



Claim Case Study: Construction

How Cowbell helped the policyholder
recover quickly with minimal loss



What happened?

- The policyholder saw that a bad actor was spoofing their email domain to send fraudulent payment requests internally
- Upon discovering the incident, the policyholder immediately notified Cowbell of the incident.

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.

Who was the victim?

Incident Type: Email Compromise

Revenue: \$30,000,000

Employee Count: Less than 100

This case study provides an overview of the claims process at Cowbell.

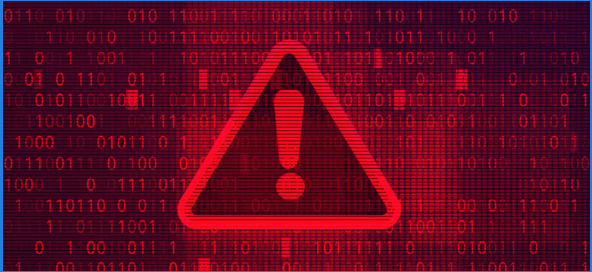
No matter the size of your business, a standalone cyber insurance policy is essential when it comes to establishing cyber resilience.

Ask your agent about Cowbell today.

Email security remains one of the most important aspects of cybersecurity for organizations. According to the Email Security Risk Report 2024 provided by the email security provider Egress, 94% of cyber decision-makers had to deal with a phishing attack in 2023.

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.

Need cybersecurity support? Contact our team at cybersecurity@cowbellcyber.ai for tailored support to make your organization as secure as possible.



Are you experiencing a cyber incident?
Report now! Call **(833) 633-8666** or email
claims@cowbellcyber.ai.

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 Cybersecurity Services team is available to advise you on cybersecurity measures to implement and how to take advantage of all resources provided.