CASE STUDY

Racing against the clock to recover $1.3M from a phishing attack

INDUSTRY
Early Childhood Education

EMPLOYEES
1–25

COVERAGES
- Funds transfer fraud
- Breach response

This nonprofit institution for childhood education learned a lesson when threat actors secretly compromised the finance director's email account. Four months passed as the attackers searched the policyholder's mailboxes for terms related to finance, banking account information, payment, and funds requests. Next, the attackers set up rules to move a series of legitimate emails from the policyholder's inbox to their junk folder.

The attacker spoofed the nonprofit's legitimate domain, configured email rules to divert replies, and sent compromised attachments. They sent an email to six people facilitating two very large fund transfers of roughly $620,000 each — totaling nearly $1.3 million. The subject line was "Change banking service," citing COVID-19 as the reason.

Shortly after the payments were made, employees received emails requesting gift cards. Additionally, the policyholder did not receive proper confirmation of funds received. The policyholder quickly realised an event had occurred and reached out to the Coalition Incident Response (CIR) team. CIR sprung into action, changed the passwords of the compromised account, and forced a global password reset.

Shortly after the payments were made, employees received emails requesting gift cards. Additionally, the policyholder did not receive the proper confirmation of funds received that they were familiar with. They knew something was wrong.

Coalition's Claims team coordinated with law enforcement to file a report and stop the funds from being transferred. CIR also put in a takedown request to remove the fraudulent domain, preventing the policyholder from receiving additional fraudulent emails from that domain. Due to our swift response, we managed to claw back all of the money except $500.

Coalition provides Active Risk Assessment of an organisation's real-time cyber risk, Active Protection through continuous threat monitoring, and Active Response to incidents if they occur — providing broad insurance coverage to solve cyber risk.

Coalition brings together active monitoring, incident response, and comprehensive insurance to mitigate the impact of cyber incidents. To learn more, visit coalitioninc.com/uk-cyber.