Mitigating Risk and Preventing Advanced Email Attacks with an AI-Based Solution

As a global leader in specialty insurance, mortgage insurance, and reinsurance, Arch Insurance has a mission to protect clients from known risks and emerging threats. The company also provides cyber insurance for clients seeking to minimize the risk of losses related to data breaches, ransomware, business email compromise, and other digital threats that arrive via advanced email attacks.

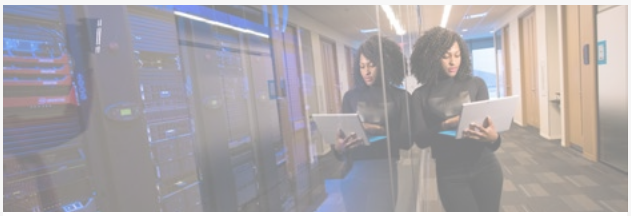
To support that goal, Arch Insurance continuously seeks strategies and solutions that could help mitigate risk for their clients. "Ransomware and BEC are two of the largest triggers for claims, and those typically come through email," said Kyle Lutterman, AVP of Cybersecurity Risk Engineering. "So, the cybersecurity underwriting challenge we have is determining which clients have good security and quality control procedures."

The Arch Insurance team found that Abnormal's behavioral intelligence capabilities and its quick, API-based integration with cloud email platforms make it a highly effective, easy-to-use risk reduction solution.

"We like that Abnormal can complement or supplement other email security tools," said Shiraz Saeed, VP of Cyber Risk. "Users don't have to switch providers to benefit from Abnormal's AI-based threat detection. It improves their existing security programs."

> "We like Abnormal because the platform uses machine learning and artificial intelligence to screen and block malicious emails. That protects the business and improves productivity, which improves the top line and the bottom line."

Shiraz Saeed
VP of Cyber Risk



Industry
Insurance

Location
Bermuda

CHALLENGES

- Continuously monitor the market for emerging solutions that reduce their risk profile without adding burdensome overhead.
- Strengthen security to avoid losses caused by increasingly advanced email threats.
- Enhance cybersecurity controls and security program maturity for better rate and coverage options.

BUSINESS IMPACT

- Advanced protection against email attacks launched from compromised vendor and employee accounts.
- Partnership that strengthens position as a leader in cybersecurity risk mitigation.
- Potential to minimize losses related to attacks on clients.

200+ High-risk vendors identified, based on vendor compromise and/or vendor impersonation seen in the Abnormal community.

Types of Advanced Attacks Prevented by Abnormal

Credential Phishing
73%
of advanced email attacks

BEC & Impersonation
$2.4B
losses in 2021

Malware
76%
of ransomware delivered via email

Account Takeover
26%
of companies targeted weekly

Fraud & Extortion
$90K
average loss per incident