SubRosa Prevents Business Email Compromise, Averting Financial Loss

A Case Study

subrosa

Contents

subrosa

Business Email Compromise (BEC) attacks have rapidly escalated into a billion-dollar criminal enterprise, with manufacturing organizations increasingly at risk. These schemes use deceptive emails that impersonate trusted executives or partners, instructing finance teams to approve fraudulent payments. Unlike many cyber threats, BEC relies heavily on social engineering and organizational awareness gaps—making it harder to detect through traditional security tools.

For manufacturers, the urgency of daily operations, the prevalence of remote supplier relationships, and the complexity of financial transactions create an environment where such fraudulent requests can slip through the cracks. This case study highlights how SubRosa, a dedicated cybersecurity solutions provider, intercepted a BEC attempt at a mid-sized manufacturing company and protected them from significant financial and reputational harm.

The Attack

A mid-sized manufacturer known for producing specialized machinery found itself in the crosshairs of a targeted BEC attack.

The scammers conducted thorough reconnaissance, gathering details about the company's executive leadership, invoicing cycles, and common payment workflows. Once they felt prepared, the attackers impersonated the organization's Chief Financial Officer (CFO), sending an email to the Accounting Manager requesting a substantial wire transfer to a "new vendor."

The email was meticulously crafted to appear genuine:

- **Familiar Tone:** It mimicked the CFO's usual phrasing and sense of urgency.
- **Accurate Formatting:** The email signature replicated official company branding, complete with correct job titles and contact information.
- **Invoice Reference:** The attackers mentioned a real invoice number that had appeared in a previous legitimate transaction, leading finance staff to believe it was an unpaid vendor.
- **Time-Sensitive Request:** The message urged the finance team to expedite the transfer due to an "urgent order," reducing the likelihood of thorough internal verification.

Attack Summary

At first glance, there was little reason to suspect foul play. The request arrived from an email address that looked nearly identical to the CFO's legitimate account—only a single character was different. In a busy manufacturing environment, where daily operations and supplier management demand constant attention, such minor discrepancies can be easily overlooked.

Case Example: A Realistic Ransomware Scenario

SubRosa had been engaged by this client to provide end-to-end cybersecurity monitoring and incident response. When the impersonation email arrived, a series of protective measures and expert human analysis kicked into action:

1

Behavioral Anomaly Detection
SubRosa's advanced email security filters flagged the message for unusual language patterns and geolocation inconsistencies. The CFO's real account typically showed a login history limited to the company's HQ and a few known travel destinations. However, the malicious request originated from an unfamiliar IP address on a different continent.

Incident Triage and Analysis
Upon receiving an automated alert, SubRosa's incident response team immediately examined the email headers, sender reputation, and domain. Their specialists also reviewed the CFO's previous communications for comparison. Discrepancies in tone, content, and sign-off times led the team to classify the email as a high-risk event.

2

3

Immediate Client Engagement
Within minutes, SubRosa notified the client's designated security liaison in the IT department, advising them to halt any scheduled wire transfers linked to this request. SubRosa's team then walked the finance department through a quick verification process, discovering the vendor was not an approved supplier and the banking details were suspicious.

Preventive Measures and Forensic Steps
SubRosa's experts rapidly disabled the compromised email alias and quarantined any related emails or attachments. Following the isolation of the suspicious account, digital forensics efforts began to trace the attacker's methods. This investigation provided valuable intelligence on how the adversary had gained access to internal details, which would inform future defenses.

4

The Result

SubRosa's timely intervention prevented the manufacturer from transferring a potentially large sum to a fraudulent account, thus averting both immediate and long-term consequences:

Zero Financial Loss

No funds left the company, avoiding what could have amounted to a tens- or even hundreds-of-thousands-of-dollars loss.

Preserved Trust and Morale

Avoiding a successful BEC attempt reinforced internal confidence in leadership, especially for the CFO and finance team. A major incident would have dampened employee morale and possibly attracted unwanted regulatory scrutiny.

Operational Continuity

By preventing the fraud at an early stage, the company kept its production and delivery schedules on track without being bogged down by investigations or potential lawsuits.

Roadmap for Strengthened Security

SubRosa offered comprehensive post-incident consulting, helping the client bolster its overall security posture—minimizing the risk of similar threats in the future.

Key Takeaways

Layered Security is Essential

Traditional email filters and antivirus software can miss sophisticated BEC attempts. By employing behavioral analytics and real-time threat intelligence, organizations gain the depth needed to detect subtle signs of impersonation—such as domain similarities, unusual sending patterns, or suspicious login locations.

Rapid, Cross-Functional Response Makes All the Difference

Speed is critical when dealing with BEC. Having a well-defined communication protocol between IT, finance, and senior management can thwart an attack before a single cent leaves the company. In this incident, SubRosa's direct line of communication with the client's IT and finance teams was a decisive factor.

Effective User Training and Verification Protocols

End users—especially those managing payments—remain a primary line of defense. Training staff to question emails requesting large or urgent transfers, and establishing secondary verification procedures (e.g., calling the supposed sender) significantly reduces BEC susceptibility.

Incident Aftermath is an Opportunity for Growth

A near-miss can be a valuable wake-up call. Implementing new safeguards—such as Multi-Factor Authentication for executives and refined vendor onboarding workflows—helps transform a dangerous incident into a catalyst for stronger overall security.

Continuous Improvement and Visibility

BEC tactics evolve rapidly. Ongoing vulnerability assessments, frequent policy reviews, and staying alert to emerging threats maintain the defense over time. SubRosa's incident follow-up reinforced the client's commitment to ongoing improvements, ensuring they remain one step ahead of future attacks.

Our Company

We deliver cutting edge security technology solutions and services to our Clients so that they are prepared to tackle the ever growing cyber threat. Through the SubRosa Unified Risk Platform, we deliver threat intelligence, security controls validation and incident alerting and response. We employ and partner with some of the leading risk and security experts in the industry, enabling us to deliver effective services and software solutions to our clients of all sizes, across the globe.

More resources available at: https://subrosacyber.com

SUBROSA
2000 Auburn Dr
Ste 200 #366
Beachwood OH
44122
888.893.1983
info@subrosacyber.com

Since 2017 SubRosa proudly delivers cyber risk advisory and related services to public, private and government clients.

This brochure is to be used as a reference for general information only, and no content contained herein is designed to provide cyber risk professional advice or services.