North Risk Partners®

XIGENT
Result Driven IT

BUSINESS EMAIL COMPROMISE: HOW TO PROTECT YOUR ORGANIZATION

JUNE 2025

NORTH RISK WEBINARS | 2025

PRESENTER

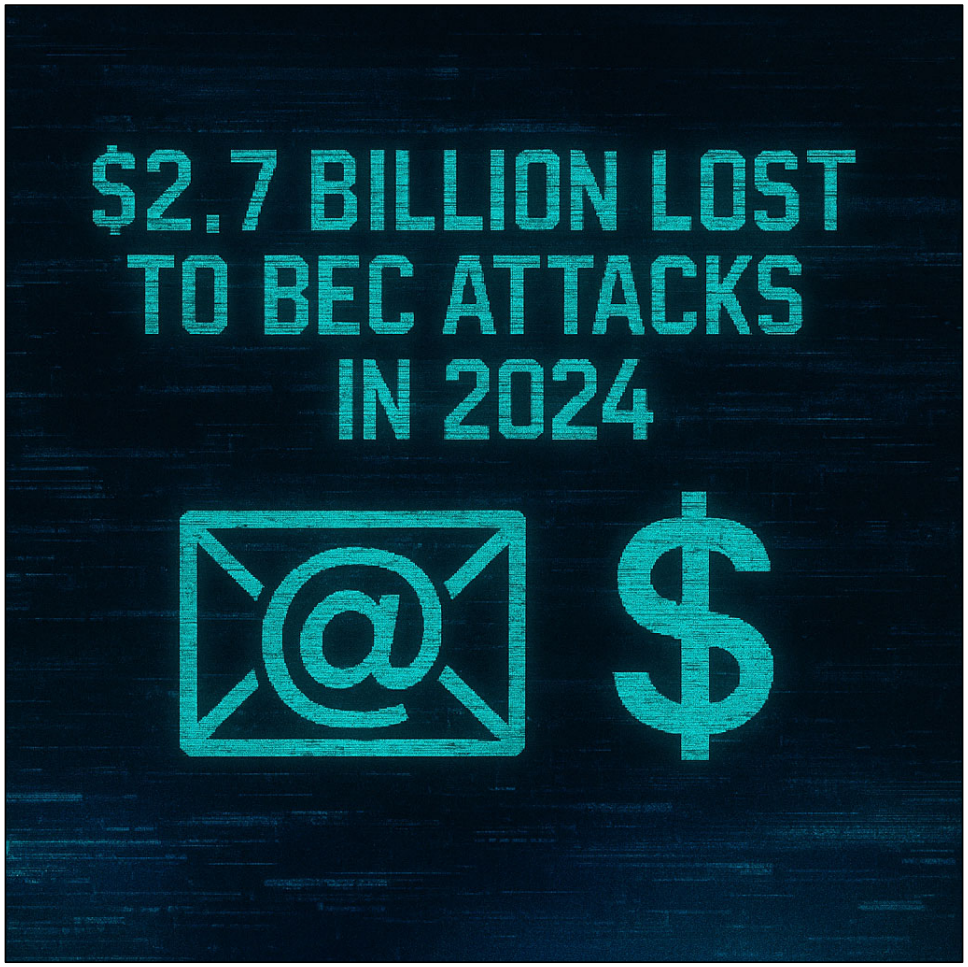
Amos Aesoph

Chief Information Security Officer

Xigent

North Risk Partners®

XIGENT
Result Driven IT


$2.7 BILLION LOST
TO BEC ATTACKS
IN 2024

WHAT IS BEC?

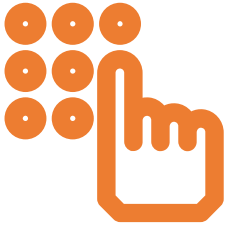
- Definition of Business Email Compromise (BEC)
- Difference between BEC & Phishing or Ransomware

Common BEC Scenarios

- CEO/CFO impersonation
- Vendor email compromise
- Payroll diversion
- Gift card scams

HOW BEC ATTACKS WORK & ATTACK LIFECYCLE

Reconnaissance



Credential Compromising or Spoofing

Social Engineering & Message Crafting

Fraudulent Communication & Fund Redirection

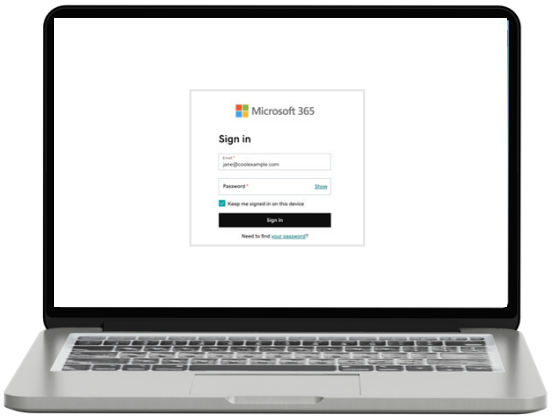
CASE STUDY: BEC ATTACK ON A MID-SIZED MANUFACTURING FIRM

- 150-employee manufacturing firm
- U.S. headquarters with overseas suppliers
- Relies heavily on email for invoice approval and payment workflows

CASE STUDY: BEC ATTACK ON A MID-SIZED MANUFACTURING FIRM

The Attack

- Compromised CFO's email account using a phishing email mimicking a Microsoft 365 login page
- Spent two weeks observing internal communications to identify payment patterns
- Sent a fraudulent but convincing email to accounts payable
- Urgent wire transfer request
- Claimed vendor banking details had changed due to a merger
- Included correct vendor name, invoice number, and dollar amount
- Accounts payable completed the transaction without secondary verification



CASE STUDY: BEC ATTACK ON A MID-SIZED MANUFACTURING FIRM

The Impact

- $147,000 transferred to an attacker-controlled offshore account
- Fraud discovered ~48 hours later after real vendor inquired about missing payment
- Funds unrecoverable
- Cyber insurance only covered $80,000 due to lack of documented secondary approval process

CASE STUDY: BEC ATTACK ON A MID-SIZED MANUFACTURING FIRM

Key Lessons Learned

Technical Controls Alone are Insufficient:

- Antivirus and email filtering didn't stop the phishing attack; MFA was not enabled

Business Process Controls Matter:

- No out-of-band confirmation for changes in vendor payment instructions

Cyber Insurance Has Conditions:

- Missing or undocumented security practices can lead to reduced or denied payouts

Social Engineering Is Highly Effective:

- Attackers exploited trust and timing, not malware

WHY BEC IS SO EFFECTIVE?

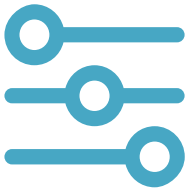
Why it is Effective

- Human Trust and Urgency
- Lack of Multi-Factor Authentication (MFA)
- Poor Email Authentication (SPF, DKIM, DMARC)
- Insider Knowledge from Reconnaissance or Breach

Red Flags to Watch For

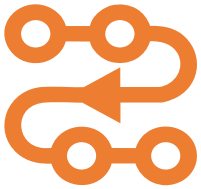
- Unusual or urgent requests
- Changes in payment instructions or account info
- Domain name lookalikes (e.g., amaz0n.com)
- Tone or timing inconsistencies
- Messages outside normal workflow

WHY BEC IS SO EFFECTIVE?



Technical Controls

- Implement MFA, especially for email accounts
- Configure SPF, DKIM, and DMARC
- Email filtering and anomaly detection tools
- Monitor for credential reuse and data leaks



Business Process Controls

- Require out-of-band verification (phone call, internal system)
- Segregation of duties for financial approvals
- Set limits and review procedures for wire transfers

User Awareness Training

- Regular phishing simulations
- Promote reporting with tools like the Phish Alert Button
- Encourage a “pause and verify” culture

WHAT TO DO IF YOU SUSPECT BEC

Immediate Steps

- Notify IT/Security Team
- Contact bank or payment processor
- Change compromised credentials
- Incident Response Plan & Legal Considerations
- Reporting to Authorities (e.g., FBI IC3)

KEY TAKEAWAYS

- How Business Email Compromise (BEC) attacks unfold
- Red flags to watch for
- Key security measures to have in place
- Recognize and prevent BEC threats
- Real financial and insurance impacts of BEC
- Practical steps you can take to protect your business

QUESTIONS?