Office of the State Auditor | Joseph M. Maestas, P.E., C.F.E., State Auditor | April 22, 2024

Risk Advisory 2024-01

Business Email Compromise

Executive Summary:

The Office of the State Auditor (OSA) continues to receive reports related to information technology security breaches resulting in material or potential losses to school district and other local government finances. These entities are often in small, rural communities. The OSA has seen the increase in what is termed “business email compromise” fraud schemes in the information security world. The purpose of this Risk Advisory is to educate entities of the scheme, provide a real-world example, provide mitigation recommendations, and provide links to other resources.

What is a Business Email Compromise Fraud?

Fraudsters engaging in business email compromise specifically target businesses and governments that are conducting payments electronically via wire transfer, and are often carried out through email addresses from administrators or executives within the organization. The fraudster will seek access to sensitive business information or seek to initiate an electronic funds transfer

How does the business email compromise fraud attack the organization?

Often the fraudster spoofs an Executive’s or Supervisor’s email or gains access to that legitimate email through implanting a trojan horse on the email network and gaining access to the email servers. The fraudster will often target finance administration professionals and ask to wire funds to pay an invoice, change bank account information on funds transfers to legitimate vendors (often accompanied by a fraudulent change of vendor information form), or ask for purchasing card information. The resulting fraudulent transfer and data breach can result in a significant loss of taxpayer dollars and distrust from the taxpaying public. Commonly, fraudsters will ask to initiate transfers of funds, tax-related material like personally identifiable information about employees, to submit fraudulent returns, or use the compromised email addresses to send fraudulent emails to vendors. Any government working with vendors that receive payment by electronic funds transfer (EFT) should consider these attacks when establishing information security controls.

New Mexico School District Example

In late 2023, a medium-sized school district had a mid-level administrator targeted with a spear phishing attack (e.g. a targeted administrator’s email with virus-laden link), compromising the email server. The emails were combed for vendor data, and when one was found it was forwarded to a spoofed vendor email address. The original email was doctored and forwarded under the mid-level administrator’s legitimate email address to their staff to route to the finance department for payment. The finance department initiated the approximately $1.4 million request by making the necessary changes in the accounting information system and did not follow the procedures to verify verbally with the vendor. The automated clearing house (ACH) prenotification prior to the electronic funds transfer was questioned by the bank. The school district was made aware of the attack in late March of 2024 following an inquiry from the bank and subsequent vendor contact, and notified OSA.

Recommendations: How to Protect Against Business Email Compromise

- Comply with State Executive Order 2024-011. Implement cybersecurity, information security, and privacy policies and procedures based upon the moderate-impact security control baselines, frameworks, and standards issued by the National Institute of Standards and Technology (NIST).
- Institute information security controls. Controls like email filters, two factor authentication, external traffic management and continual quality improvement on information technology controls can be implemented. IT staff should be conducting vulnerability assessments, have an intrusion detection system that flags domains that mimic contracted vendors or the government entity, block sites that are known to spread viruses, and should keep software and virus scanning patches current. Vendors should have verifiable cybersecurity measures.
- Implement staff information security policies and procedures. These should include not clicking on external links, verbal confirmation of banking changes, vendor confirmation on all payment information changes, and limits on transfer amounts or requiring secondary approvals.
- Know your high-risk fraud targets. Fraudsters most commonly target high-level executive team members, information technology professionals, finance and administrative services staff, and administrators or executives with procurement responsibilities. Anyone with information security or accounting transaction responsibilities who has limited knowledge, skills or abilities in these areas may be at higher risk. Fraudsters are often seeking high-dollar wire transfers or sensitive employee information to file fraudulent tax returns for refunds.
- Train staff. Train staff on email security, common phishing attacks, and use up-to-date examples. Conduct simulation phishing to raise awareness and professional skepticism of staff.
- Look for fraud indicators. Fraudsters attempt to compromise staff by creating a sudden, false sense of urgency. According to the Federal Bureau of Investigation (FBI), commonly the fraudsters will use the phrases “code to admin expenses” or “urgent wire transfer”. For wire fund fraud, often the fraudulent bank may be located overseas.

Sources:

Governor’s Executive Order 2024-011 Strengthening Cybersecurity https://www.governor.state.nm.us/wp-content/uploads/2024/04/Executive-Order-2024-011.pdf

Knowbe4 CEO Fraud https://www.knowbe4.com/ceo-fraud#

FBI Alert Number I-061416-PSA https://www.ic3.gov/Media/Y2016/PSA160614

FBI’s Business Email Compromise website https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise

NIST Cybersecurity Framework Website https://www.nist.gov/cyberframework

OSA
GAO

Related Past OSA Risk Advisories:

Risk Advisory: OSA Fraud Alert: “Smishing” Scam, July 21, 2021. https://www.osa.nm.gov/wp-content/uploads/2021/07/Risk-Advisory_MVDSmishingScam.pdf

Risk Advisory: Don’t Get Spoofed: Payroll Phishing Fraud Alert, March 4, 2019 https://www.osa.nm.gov/wp-content/uploads/2019/06/Spoofed_Email_3-4-19.pdf

Risk Advisory: Phishing E-mail Targets Schools, September 18, 2018 https://www.osa.nm.gov/wp-content/uploads/2019/06/GAO-Risk_Advisory-CharterSchoolPhish-2018-09-18.pdf