6 Key Components of A Company Business Email Compromise (BEC) Policy

In today's digital landscape, businesses face numerous cybersecurity threats, with email-based attacks being among the most prevalent and damaging. Business Email Compromise (BEC) is a sophisticated form of cybercrime where attackers impersonate high-level executives or trusted partners to manipulate employees into transferring funds, disclosing sensitive information, or executing malicious actions. To safeguard against this threat, companies must develop comprehensive BEC policies. A business email compromise policy can guide and allow employees to feel safer by following pre-defined rules. Here are six essential components that every BEC policy should include:

1. **Employee Awareness Training:** The first line of defense against BEC attacks is a well-informed and vigilant workforce. Employee awareness training should cover the various forms of BEC scams, including impersonation tactics, invoice fraud, and CEO fraud. Employees must understand the importance of verifying the authenticity of email requests, especially those involving financial transactions or sensitive information. Training should also emphasize the importance of reporting suspicious emails promptly and provide clear guidelines on how to do so. Security awareness training should be stipulated by the BEC policy as a key component for employee onboarding and regular trainings.

2. **Authentication Procedures:** Implementing robust authentication procedures is crucial for preventing unauthorized access to company email accounts. Multi-factor authentication (MFA) should be enforced for all corporate email accounts to add an extra layer of security beyond passwords. Additionally, companies should regularly review and update their list of authorized email users, promptly revoke access for former employees, and implement strong password policies to reduce the risk of account compromise.

3. **Verification Protocols for Financial Transactions:** BEC attacks often target employees responsible for financial transactions, such as accounts payable or finance personnel. To mitigate this risk, companies should establish strict verification protocols for all financial transactions initiated via email. These protocols may include requiring dual authorization for fund transfers above a certain threshold, implementing a call-back procedure to verify payment requests, and cross-referencing banking details with known vendor information.

4. **Supplier and Vendor Validation:** Attackers frequently exploit relationships with trusted suppliers or vendors to perpetrate BEC scams. Therefore, companies should conduct thorough due diligence when onboarding new suppliers or updating payment information. This may involve verifying the legitimacy of supplier contacts through independent channels, such as official websites or phone calls to established numbers, rather than relying solely on email communication. Additionally, companies should establish clear procedures for validating and authorizing any changes to vendor payment details. Never change payment or banking details based on an email request alone.

5. **Open-door Reporting:** Organizations should work hard to develop a policy, culture, and set of processes that make it easy for employees to report requests incidents that feel off to them — even if they've already made mistakes. It's critical as you establish a security first culture that employees are not scared to report an incident or questionable action

they may have taken. The sooner something is reported the easier it is to address, but scared employees may not want to admit mistakes. The idea is to set up documented steps and mechanisms for reporting and to try to reward thwarted mistakes more than the organization punishes mistakes. Try adding incentives such as a gift card or recognition for those that successfully identify and thwart attempted BEC attacks. This will help foster a defensive mindset and zero trust mentality and they need to know how to do this safely.

6. **Incident Response Plan:** Despite proactive measures, BEC attacks may still occur. Having a robust incident response plan in place is essential for minimizing the impact of such incidents and facilitating a swift recovery. The plan should outline the steps to be taken in the event of a suspected or confirmed BEC attack, including isolating affected systems, notifying relevant stakeholders, and engaging law enforcement or cybersecurity experts if necessary. Regular testing and simulation exercises can help ensure that employees are familiar with the response procedures and can act decisively in a crisis.

A comprehensive BEC policy is essential for protecting businesses from the ever-evolving threat of email-based cybercrime. By incorporating these six key components into your policies, companies can bolster defenses against BEC attacks and mitigate the risk of financial loss, reputational damage, and data breaches. Ultimately, investing in proactive cybersecurity measures is critical for safeguarding the integrity and resilience of modern businesses in an increasingly digital world. *For questions or a cybersecurity assessment, reach out to Computer Dimensions today @ 520-743-7554.*