Commercial Risk Advisor

Vendor Email Compromise

APEX BENEFITS PARTNERS
where clients come first

As businesses rely more heavily on vendors for operations and growth, cybercriminals have found new ways to exploit these trusted relationships. One emerging tactic, vendor email compromise (VEC), involves impersonating a legitimate supplier or partner to steal data or divert payments. While business email compromise often involves impersonating internal executives or employees, VEC focuses specifically on external partners, vendors and suppliers, making these attacks extremely difficult to detect.

How Vendor Email Compromise Works

VEC attacks are built on social engineering and trust exploitation. Attackers may:

- Access a vendor's account using phishing or stolen credentials.
- Gather intelligence on payment schedules, key contacts and communication tone.
- Monitor email traffic with hidden forwarding rules.
- Launch fake payment requests that appear legitimate, often during routine invoice cycles.

Victims might not realize they've been targeted until payments are diverted or sensitive information is exposed.

Why These Attacks Succeed

These scams thrive because they closely mimic routine vendor communications, referencing real transactions, matching normal timing and using legitimate-looking addresses. Because many VEC attacks originate from a vendor mailbox that has already been compromised, traditional email filters and authentication checks may not detect them. The fallout can be severe, leading to financial losses, operational disruptions, regulatory scrutiny and lasting reputational harm.

How to Protect Your Business

Mitigating VEC risk requires a multilayered defense strategy:

- Strengthen technical safeguards by using authentication protocols such as SPF, DKIM, and DMARC to verify email senders. These controls help reduce spoofing but may not block attacks sent from a compromised vendor account.
- Use behavioral monitoring tools that apply artificial intelligence to flag unusual message patterns or tone changes.
- Verify vendor requests by confirming payment or account changes through a phone call or secure portal rather than relying on email alone.
- Monitor vendor security through regular reviews and by requiring partners to maintain strong cybersecurity standards.
- Train employees with scenario-based exercises to help them recognize and report suspicious communications.

Insurance Considerations

Both cyber and crime insurance can help offset losses from VEC incidents, but coverage details vary as follows:

- **Crime policies** with social engineering fraud endorsements often cover direct financial losses from deceptive payment instructions.

- **Cyber policies** typically address data exposure, legal costs and breach response.

Because social engineering fraud and funds-transfer losses may be subject to specific conditions, exclusions or low sublimits, it's essential to review policy wording closely. Working with a knowledgeable insurance professional ensures these policies complement one another and provide the right protection.

The Bottom Line

Vendor email compromise is one of today's most sophisticated cyber threats. Staying vigilant, maintaining strong vendor-management practices and verifying all payment changes are critical steps toward prevention.

Contact the insurance professionals at Apex Benefits Partners to review your cyber and crime coverage and ensure your business is protected against evolving cyber risks.

Best Practices for Developing a Climate Action Plan

As climate-related risks grow, more businesses are taking proactive steps to reduce their carbon footprint and strengthen resilience. A climate action plan (CAP) helps organizations outline measurable goals for cutting emissions, improving efficiency and adapting to changing environmental conditions. It also demonstrates accountability to stakeholders and can support compliance with evolving regulations.

What Is a CAP?

A CAP serves as both a roadmap and a commitment to reduce greenhouse gas (GHG) emissions while preparing for climate impacts. Most plans include an emissions baseline, reduction targets, timelines and action steps across energy, transportation, waste and procurement. When integrated into business strategy, CAPs can enhance efficiency, attract investors and improve long-term sustainability.

Steps for Developing a CAP

Creating an effective CAP requires data-driven decisions, clear objectives and input from across the organization.

- **Assess the carbon footprint**. Start by calculating current GHG emissions from direct operations, purchased energy, and other indirect sources, such as business travel and supply chain activity. This baseline helps identify major contributors and reduction opportunities.
- **Set measurable targets**. Establish science-based, time-bound goals that align with global agreements such as the Paris Agreement. Make targets public to reinforce transparency and accountability.
- **Create a decarbonization roadmap**. Outline actions for meeting these targets, such as transitioning to renewable energy, electrifying fleets and improving efficiency. Assign responsibilities, set milestones and allocate resources for implementation.

Key Focus Areas

Effective CAPs target high-impact areas of operations:

- **Energy and efficiency**—Upgrade to energy-saving systems and renewable sources.
- **Supply chain**—Partner with vendors committed to sustainable practices and emissions tracking.
- **Employee travel**—Promote carpooling, public transit, remote work and electric vehicle adoption.
- **Waste reduction**—Implement recycling and composting programs, and move toward paperless workflows.
- **Climate resilience**—Assess vulnerabilities and update business continuity plans to address extreme weather risks.

Putting the Plan Into Action

Implementation is critical. Educate employees, engage leadership and collaborate with suppliers to reduce emissions across all levels. Integrate sustainability goals into company governance and risk management, track results through standardized frameworks and share progress openly. Regular audits, third-party verification and annual updates keep plans credible and responsive to new technologies and regulations.

A strong CAP is more than an environmental initiative; it's a smart business strategy that builds resilience and long-term value. For more risk management guidance, contact us today.
