Protecting Organizational Vulnerabilities from Cyber Crime

While the periodic multi-million ransomware attacks get viral headlines, a far more pervasive cyber threat quietly drains millions from organizations every day. Social engineering attacks—particularly those targeting emails—have become the favored tool of threat actors. According to a recent survey, 79% of organizations were victims of cyber-attack attempts and events in 2024, down a mere one percent from 2023.[1] Attacks are happening globally every day, costing $10.5 trillion, and it's taking a toll on organizations, whether they are a global corporation or a 100-person organization.

THE ART OF DECEPTION

Social engineering is manipulating emotions. The goal of a social engineering attack is to trick people into sharing information they shouldn't share, downloading software they shouldn't download, visiting websites they shouldn't visit, sending money to criminals, or making other mistakes that compromise their personal or organizational security.[2] Threat actors prey on an employees' natural tendencies to please their bosses, meet deadlines, and maintain good business relationships.

Phishing is one of the more common scams that threat actors use when engaging in a social engineering scheme. These scams are digital text or voice messages crafted to look or sound like they come from a trusted individual or a credible organization, one the recipient has a familiar relationship with.[3] There are several variations of phishing attacks, including:

+ **Whaling** specifically targets executives, exploiting hierarchical relationships and the authority that comes with C-suite requests.
+ **Spear phishing** gets personal, using individual information gleaned from social media or data breaches to craft believable, targeted messages.
+ **Smishing** brings these tactics to text messaging, catching people off guard on their personal devices.

PHISHING: UNDERSTANDING THE TACTICS

Email has evolved into a central hub for modern business operations, a gateway to banking portals, vendor management systems, customer databases, and countless other critical platforms. Threat actors combine phishing scams with social engineering techniques with the hope of snaring an unsuspecting employee into tapping a link that gives them access to an organization's digital systems. Insurers refer to successful phishing attacks committed through email as business email compromise (BEC), which, along with funds transfer fraud (FTF), are the top two cyber claims filed, according to Anne Juntunen, claims specialist with Coalition Insurance.

Business email compromise aims to lead to a funds transfer fraud," Juntunen said on a recent IMA and Coalition cyber webinar. "Even when a threat actor isn't able to achieve this goal of the illegal funds transfer, they can still do a lot of damage with a person's email."

When threat actors gain control of legitimate employee email accounts, they use this access to perpetrate fraud against their victims' colleagues or third-party vendors or clients, even inducing them into sending money to the threat actor, according to Bret Ommodt, IMA Cyber Claims Specialist.

OPERATIONAL DISRUPTIONS AND MONETIZING VULNERABILITIES OR MONETIZED DISRUPTIONS

Threat actors are particularly interested in employees with privileged access to financial systems, but even compromising a low-level account can provide the intelligence needed for a devastating attack. Suppose an attacker successfully gains a foothold in their victim's email. In that case, they can observe communication patterns, understand payment schedules, and wait for opportunities—perhaps when key personnel are traveling or during busy periods when routine procedures might be relaxed. BEC allows threat actors to access a system, and FTF is when an employee or vendor is tricked into sending money to a fake account.

"The more access that a threat actor has to the system, the more likely and more quickly they're able to perpetrate this kind of fraud," Ommodt said on the IMA-Coalition webinar.[4] ***"It goes back to the added element of what a BEC is, that it's a legitimate email address people have grown accustomed to working with and they're more likely to accept change of account details via email without verifying them, if it's from an email address that they work with on a weekly or daily basis."***

The statistics paint a sobering picture. According to Juntunen, Coalition receives roughly 5 BEC and 5 FTF claims a day, "and we're just one carrier," she cautions. A standalone BEC claim averages $35,000, but the average loss increases up to $185,000 when an email compromise leads to a funds transfer claim.

Case Study

A restaurant chain's recent experience illustrates how seamlessly criminals exploit trusted relationships. The company was remodeling one of its locations and had established a payment schedule with its equipment vendor—four installments for the project. The first payment, a check sent overnight, proceeded normally.

When the second payment came due, the restaurant's accounting team received an email with an invoice. Initially planning to send another check, they received a follow-up message requesting a wire transfer instead, citing urgency. The request came from what appeared to be the vendor's email address, continuing an existing conversation thread. The accounting team, maintaining good vendor relations and seeing no red flags, complied with the wire transfer request for $97,000.

Two weeks later, the vendor called asking about the missing payment.

Investigation revealed both the restaurant's email environment and the vendor's personal email had been compromised. The threat actors had been monitoring communications, understood the payment schedule, and struck at the perfect moment. They didn't need to create an elaborate false identity—they simply inserted themselves into an existing, trusted business relationship.

THE INSURANCE SAFETY NET

When these attacks succeed—and they do with alarming frequency—proper insurance coverage becomes critical. According to Ommodt, cyber and crime insurance are the most applicable coverages to these types of events and provide the best avenues for recovery. These policies typically address social engineering fraud, funds transfer fraud, and phishing-related losses, covering both direct losses and third-party impacts.

These two coverages are not the only opportunities for insureds to recover losses through their insurance. Liability coverages such as management, D&O, employment practices, and errors and omissions can provide sublimits that are applicable to social engineering or funds transfer fraud. According to Ommodt, tapping into these coverages can provide relief from $25,000 up to $100,000, depending on policy and carrier, but when the fraud is in the hundreds of thousands of dollars, "you want to explore every opportunity for recovery."

Ommodt cautions that insureds need to review what their cyber policy covers, as cyber insurance is non-standard across providers of cyber insurance. He said organizations must understand how their cyber and P&C coverages apply to a cyber event before an incident occurs. This is also an important consideration when considering a carrier change. What one carrier covers regarding BEC or social engineering, for example, another may not – both will likely have different limits. Policies are also likely to differ in the risk management protocols they require.

Beyond financial recovery, a comprehensive cyber policy often provides access to forensic experts who can determine the breach's extent, legal counsel to navigate notification requirements, and IT resources to prevent future incidents. This support proves invaluable when dealing with compromised vendor relationships and potential regulatory obligations.

BUILDING YOUR DEFENSE

While insurance provides essential protection, prevention remains the best strategy.[5] Multi-factor authentication has evolved from recommendation to requirement—any system that supports it must have it enabled. For financial transactions, implement additional verification layers: always confirm payment changes through previously verified channels, never through email. Consider prohibiting financial updates via email entirely.

Create and enforce callback procedures for all payment changes, using predetermined contacts and phone numbers established during vendor onboarding. Ensure multiple employees verify significant transactions, especially when normal approvers are unavailable. Conduct regular security awareness training that includes simulated attacks—better to fail a test than fall for the real thing.

As artificial intelligence makes these attacks more sophisticated and harder to detect, the irony is that our best defenses often involve decidedly analog solutions. Pick up the phone. Verify through separate channels. Trust but verify. In an age of deepfakes and AI-generated communications, human connection becomes a necessary layer of protection.

The Path Forward

Building a cyber defense is about instilling organizational resiliency that protects not only the organization but also its personnel, vendors, and clients. From client relationships to privacy issues, the ripples of one cyber event can create waves of damage, especially if threat actors' activities remain undetected.

The threat landscape will continue evolving, and a cyber-attack can debilitate an organization. Resiliency is key, and it starts with understanding current and future risks while implementing the necessary protocols, including the right insurance for your situation. Working with an experienced cyber carrier or broker is an investment with a trusted partner who can help navigate an ever-changing risk landscape.

LEARN MORE ABOUT CYBER CRIME TRENDS, MITIGATION, AND INSURANCE SOLUTIONS IN OUR LATEST WEBINAR

Sources:

1 AFP. (2025, April 15). *Survey: 79% of Organizations Were Victims of Attempted or Actual Payments Fraud Activity in 2024*. Association for Financial Professionals

2 IBM. (n/a). *What is social engineering?* IBM. https://www.ibm.com/think/topics/social-engineering

3 IBM. (n/a).

4 IMA Financial Group and Coalition Insurance. (2025, October 21). *Cyber Crime: Trends, Mitigation & Insurance Solutions*. IMA Financial Group, and Coalition Insurance. https://imacorp.com/insights/webinars-on-demand-cyber-crime-trends-mitigation-insurance-solutions

5 Burke, et. al. (2025, March 10). *Preparing for and Managing a Cyber Attack*. IMA. https://imacorp.com/insights/insurance-insights-preparing-for-and-managing-a-cyber-attack