Provided by Risk Strategy Solutions

RISK ADVISOR

March 2023

COMMERCIAL

Business Email Compromise Explained

Cybercriminals continue to become more sophisticated, leveraging a wide range of tactics to attack their victims. One tactic that has increased in frequency, complexity and resulting losses over the past few years is the use of business email compromise (BEC) scams. Essentially, BEC scams consist of cybercriminals impersonating an individual or entity within their targets' trusted networks for malicious gains.

There are several different types of BEC scams, including:

- **False invoice scheme**—A cybercriminal impersonates an organizational supplier to trick their target into paying fraudulent invoices or transferring funds to a phony account.
- **CEO fraud**—A cybercriminal impersonates a senior-level employee or executive and requests that their victim conduct a wire transfer to a fake account.
- **Account compromise**—A cybercriminal hacks into an employee's or executive's actual email account and distributes messages to various contacts.
- **Attorney impersonation**—A cybercriminal impersonates a lawyer or other legal representative and requests a payment be made to a phony account.
- **Data theft**—A cybercriminal impersonates an HR professional to trick their target into sharing personal information about employees or executives.

Any employee can become the target of a BEC scam, putting the security and financial stability of an entire organization at risk. Organizations can implement the following cybersecurity measures to help avoid BEC scams:

- **Educate employees.** Minimizing losses from BEC scams starts with training employees to detect and prevent such instances. This includes refraining from sharing personal or work-related information on social media, avoiding opening or responding to unknown individuals or organizations and being wary of emails that lack personalization, contain spelling and grammatical errors, request sensitive details or use threatening language.
- **Implement effective payment protocols.** Having safe and secure payment procedures within an organization can help stop BEC scams before any money is lost. Instruct employees who handle the organization's financial operations to carefully analyze invoices and fund transfer requests to ensure their validity.
- **Restrict access to sensitive data.** Only provide employees with access to sensitive organizational data if they are trusted and require such information to conduct their work tasks. Protect this data with access controls and multifactor authentication measures.
- **Utilize security features.** Make sure all organizational devices possess adequate security features to help deter BEC scams—including access to a virtual private network, antivirus and malware prevention programs, email spam filters, data encryption capabilities and a firewall. Update these security features as needed.
- **Have a plan.** Ensure the plan specifically addresses response protocols and mitigation measures for BEC scams.

For more risk management guidance, contact us today.

Cargo Theft on the Rise

Cargo thefts in the United States and Canada increased 20% from 2021 to 2022, resulting in an estimated $223 million in cargo stolen, according to Verisk's cargo theft and prevention recovery network CargoNet. The most stolen commodities were household goods (e.g., appliances, furniture, tools and toys) and electronics (e.g., computers and televisions).

Almost half of all reported cargo thefts occurred in California, Texas and Florida—with California experiencing a 41% increase in thefts year over year. This can be attributed to a significant increase in theft activity around major intermodal hubs. In fact, California is a major logistics hub for computer and green energy components, which were some of the most frequently stolen items in 2022. Georgia also saw a 34% increase year over year in cargo theft, likely resulting from the increased traffic to the Port of Savannah and the state's shutdown of its cargo theft investigation task force in 2020.

In 2022, there was a 600% year-over-year increase in fictitious cargo pickups. This fast-growing form of cargo theft involves thieves using phony credentials to pick up shipments before the legitimate carrier does and redirect them to a different address.

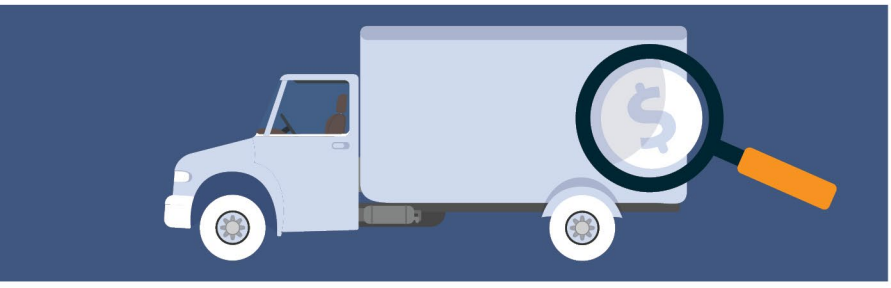
To prevent cargo theft, brokers and shippers should take the following precautions:

- Verify the name of the motor carrier and the driver with the contact information on file with the Federal Motor Carrier Safety Association.
- Vet new customers that offer payment through peer-to-peer money transfer apps prior to accepting payment and transferring goods.
- Never leave trailers loaded and unattended, especially in high cargo theft areas.
- Use high-security rear door locks and air cuff locks.
- Install landing gear locks.
- Conduct regular training and awareness events for employees.

As cargo theft becomes more commonplace, it's essential for companies to implement policies and procedures to minimize such events.

For more risk management guidance, contact us today.

Risk Strategy Solutions



In 2022, the average value of **cargo stolen** in a given event was **$214,104.**