CYBER UPDATE

Business Email Compromise Losses Increase 58%

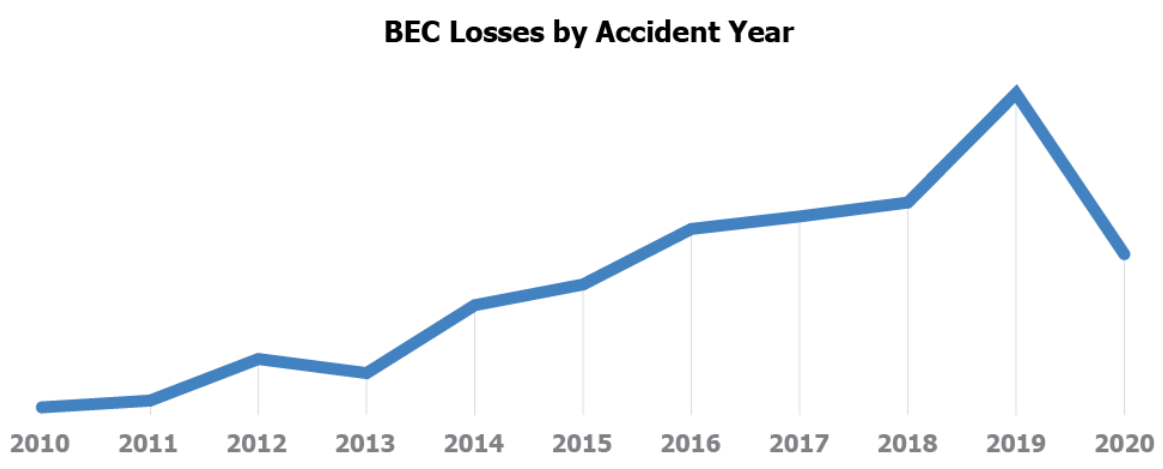
Business email compromise (BEC) losses are among the most expensive types of social engineering losses, and they are on the rise—increasing 58% from 2015 to 2019, according to Advisen loss data.

The median cost of a BEC loss is $764,000—significantly more expensive than other social engineering losses, which average around $580,000, according to Advisen loss data.

Between 2016 and 2019, there were nearly 170,000 BEC incidents reported to the FBI, accounting for over $26 billion in exposed dollar loss. Exposed dollar loss includes both actual and attempted losses.

In a BEC scam, cybercriminals send an email that appears to come from a known source making a legitimate request. Examples of this include a vendor company sending an invoice with an updated address or a CEO asking an assistant to purchase gift cards for employee rewards.

There are a couple common techniques used by scammers to trick victims into wiring payments or giving them important financial information. Scammers may spoof email accounts or website URLs with slight spelling variations in an attempt to trick employees into believing fake accounts are authentic. Scammers may send spear-phishing emails targeting specific individuals or organizations to trick victims into revealing confidential information that can be used in BEC scams. Cybercriminals may also use malware to infiltrate an organization's system and gain access to legitimate conversations about billing and invoices, allowing them to send more convincing messages to their victims, according to the FBI.



BEC losses have risen steadily over time to reach an all-time high in 2019. The drop in 2020 is likely due to a data lag and is not a reflection of an actual decrease of BEC losses.

The information sector has the highest severity of BEC losses of any industry in Advisen's loss database—nearly double that of any other industry. One of the drivers of these high losses was the Rimasauskas BEC scheme, in which Evaldas Rimasauskas targeted multinational internet companies and tricked employees into wiring money overseas. Over the course of his scheme, Rimasauskus convinced employees at Google and Facebook to transfer over $100 million into bank accounts that he controlled, according to Advisen loss data.

Even a single BEC loss event can cost tens of millions of dollars. This was the case for the Belgian bank Crelan, which lost around $75.8 million from a single spear-phishing email in 2016.

To prevent these types of losses, employee training is essential. Employees should know to check for spelling and grammar mistakes that could help reveal a scam. Employees should also be encouraged to reflect on whether an email is out of character for the sender and to be particularly wary of any email requesting action that contradicts company protocols.

Businesses can also help protect themselves by making email more secure. This can be done by adopting multifactor authentication—which increases security by requiring access to an account holder's physical device in addition to their login credentials—and utilizing business email security software to help users identify BEC attempts.

Speak with SCS Agency Inc for more cybersecurity guidance.