New Paradigm for Fighting Cyber Fraud in the Automotive and Mobility Industries

Jun 26, 2023

Categories:

Publications
Technology Blog

Authors:

William T. Repasky
Patricia Kirkwood Burgess

Business email compromise (BEC) fraud is the number one cybercrime faced by American businesses, as has been the case for years according to the FBI's Internet Crime Complaint Center's annual reports. A single BEC attack can be financially devastating and materially harm a business's reputation. For about as long as BEC attacks have been bedeviling American businesses, technology and training solutions have been the commonly prescribed remedial measures. But the problem persists and by some assessments is growing. Alternative tools must be brought out of the toolbox. This article proposes a new approach to combatting BEC fraud in the automotive and mobility industries.

While all manufacturing involves the production and delivery of goods and services for compensation, the modern mobility industry often involves distant parties with complex, interdependent supply chains and numerous intermediaries affecting the production, shipping, and payment arrangements. Cyber fraudsters see opportunities in this complexity.

The Biz of BEC Attacks

Cyber fraud takes many forms, but the species with the greatest risks are BEC attacks. The FBI's Internet Crime Complaint Center's 2022 report again listed BEC losses as the number one cybercrime in terms of dollars lost, a position it has maintained for at least the last seven years. In a typical BEC attack, a fraudster will gain access to an email account of a business's employee. Once inside the system, the fraudster secretly reads all past and future email traffic until she/he learns of a large upcoming payment. Then an email is sent to the party owing the payment, supplying fraudulent payment instructions. The employee whose email was compromised will be unaware of those communications being sent and received in furtherance of the scheme, as the fraudster typically imposes auto-

forwarding rules and the like to insure the employee remains unaware of the email traffic. Then, if the payor follows the received payment directions, the funds will be directed for deposit to a bank account controlled by the criminal, typically by wire or ACH payment. Thereafter, the fraudster will re-transfer the funds nearly immediately upon receipt, with the likely result that the funds are lost forever.

BEC attacks come in different varieties. Another common variant is known as CEO fraud. Here, a senior executive's email is hacked, but with the objective of sending a fraudulent email inside the company to someone with the accounts payable or treasury team demanding that a payment be made. Often, the fictitious email claims the payment must be made urgently and that it is a matter of secrecy the payment staff should not discuss with others.

Regardless of the method of intrusion or form of the BEC attack, a successful attack can be very expensive and often exposes the victimized company to serious reputational harm. In addition, a customer who mistakenly transfers payment faces the real risk of breaching its contract with the vendor to whom the debt was owed because it was instead paid to the fraudster.

Security vendors have entered the market space offering different technologies for hardening a company's computer servers. But, while technological options must be considered, this too often appears like a costly game of "whack-a-mole" as the hackers are always changing their attack vectors and improvising new schemes. The other commonly considered defense tactic is investing in employee training, provided a majority of BEC attacks begin with a phishing email. Training, and more training, is always appropriate but cannot guarantee a complete defense. Furthermore, with the rise of artificial intelligence and the increasing sophistication of Google Translate-type programs, the days of clumsy and grammatically suspect phishing emails are behind us. And only one employee needs to click on the bait.

It is unreasonable to expect we can ever technologically defeat or fully train our way out of BEC risks. Technology and human nature both present perpetually uncontrollable variables cybercriminals

will exploit. Thus, the question is what are other variables that businesses can actually control with some certainty to lessen the BEC risks or their consequences? A different paradigm needs to be employed or at least considered as a defense. Regardless of the facts and circumstances of the business situation, there will always be a contract through which the goods are manufactured for compensation. Contracts can be an important additional tool to shore up your company's cyber defenses.

When Your Company Is the One to Be Paid

If your business is the one to whom payment is owed under a contract, you cannot control your customers' security procedures. Nor can you direct your customers' employees to remain vigilant for the attacks that will be directed against them. But always there is a contract memorializing the parties' bargain, and this contract must be made "consequential" for all BEC purposes.

Your customers likely will face BEC attacks in the event your own company's email servers are compromised—e.g., they will receive fraudulent change in payment instructions originating from one of your "real" employees. Even the hacking of one of your trusted agents can lead to BEC attacks harmful to your business. By way of example, we handled a case where the law firm that drafted the parties' contract was hacked and was the source of the bogus payment instructions that regrettably were relied upon. Other likely attack vectors include "spoofing" emails, which your customers will receive that appear as if they emanated from your organization, along with cybersecurity breaches of the customer's own system. Regardless of the attack vector, your contracts should be drafted, and even amended, to make sure the BEC attacks do not result in your customers paying a fraudster.

We commonly recommend specific language be included in all contracts whereby (a) your payment directions and information are included in the written/preprinted terms, such as your bank routing number and account number; and (b) the customer agrees to make those payments in no other way and to no other bank. While contracts obviously differ among industries and based on the goods or services involved, there typically are standardized terms

and conditions: often the infamous “boilerplate” found on preprinted invoices, a website, or the reverse side of carbons. Therein the customer will commit to not honoring any change in payment instruction received (from anyone) via email or SMS text message and/or that the customer will not rely upon any such electronic communication setting out alternative payment directions, without first confirming the instructions’ validity through a landline call, or other out-of-band communication, to a specific person at your company named in the contract itself. This last point can be important, as our experience is that fraudsters in their BEC attacks often include a telephone number for the customer to call in case of questions regarding the newly supplied payment instructions, which telephone number is invariably linked to a call center manned by the fraudster or a criminal affiliate in furtherance of the scheme.

A contractual approach to BEC avoidance serves two primary purposes. First, it imposes a control on your customers, which we hope they will honor. Avoiding a BEC situation is the ultimate prize. Second, even if the customer’s staff ignores its contractual duty, this term will be legally beneficial in the litigation that commonly results. For purposes of this article, please accept our experience that courts facing BEC lawsuits typically adopt one of two philosophies in their adjudications. The first general school of thought is that the terms of the contract are all controlling. For these courts, a provision such as the one being recommended will be consequential. The other basic judicial approach is to resolve the dispute by a fact-finding inquiry to determine the comparative fault of the two “innocent” parties or to determine which of the parties had the last best opportunity to prevent the BEC fraud. Here again, having appropriate contractual language in place will be most beneficial in shifting the fault analysis onto the customer.

Before leaving this point, terms and conditions can both avoid some attacks and put your company in the best possible position when they do occur, but the “credit risk” of a BEC attack will remain. In short, should a customer fall victim to a fraudster’s scheme, will that customer have the financial capacity to pay your invoice “twice”? Assuming the fraudster is long gone with the customer’s funds, your

customer still faces the underlying contract to pay your company for those goods or services. This credit risk factor can be mitigated by requiring the customer to maintain insurance for such scams. This is not always practicable or appropriate, but we would be remiss not to raise for consideration this additional contractual tool in the fight against BEC attacks.

When Your Company Is the One That Owes Money

Your company's BEC bulwark should include insurance for the associated risks, contract terms, and ongoing efforts to build a culture of skepticism internally. Our experience is that building contractual defenses is problematic when our clients are the anticipated payors. Nonetheless, we have seen contract terms permitting clients to reasonably rely on electronic communications received from vendors that are then acted on in good faith. Such contractual provisions help in situations where the presiding tribunal has a history of applying a comparative fault-type of analysis. Similarly, contractually allowing your staff not to be bound by payment instructions electronically received from a vendor is often acceptable all the way around, so long as an agreed-upon verification method is memorialized and provided the verification can be expeditiously accomplished.

While the typical BEC employee training focuses on spotting phishing attempts, we believe that training aimed toward building a culture of skepticism is at least equally important, especially for all your staff who can push "send" on a payment order. A good rule of thumb is that vendors do not change banks in the middle of a contract's performance. This training focus is all the more crucial in guarding your company against CEO fraud attacks. Employees must feel empowered in confirming—through an out-of-band process—the veracity of an email supposedly coming from her or his boss requesting a payment. Again, confirmation must be done out-of-band, as it does no good for the employee to "reply" to an email received that possibly originated from a fraudster.

Often, out-of-band verification can be as simple as employees getting out of their chair and walking down the hall to speak in

person with the executive. As fraudsters can learn through social media or other sources when business leaders are unreachable due to travel or other situations, this situation must be covered in the training. There are good work-arounds for such circumstances, including a dual-control protocol. In training, we often suggest that if you are concerned you may be making a mistake, then make that mistake together, i.e., run the payment request by others before executing it. Or, as a client once said, one of the great rules of business common sense is to measure twice and cut once, which has a certain ring to it when training to create that culture of skepticism.

Business email compromise or BEC attacks have been with us for a long time and are not going away. Each can be a very expensive problem for the company. Continue to employ the best technological solutions and train your staff for the risks, but also consider all the tools in your toolbox for mitigating this severe financial risk. The core contract, wherein the benefit of the bargain between you and your vendors, customers, and other mobility industry participants is first established, can be fashioned into a valuable tool in the fight against BEC cyber fraud.

For more information or assistance, please contact the authors of this article or any attorney with Frost Brown Todd's Mobility and Data Security & Privacy teams.

FBT Gibbons