NICE
ACTIMIZE

Define - Detect - Defend: The Path to Defeating Business Email Compromise Fraud

Robert Tharle

Fraud Subject Matter Expert - NICE Actimize

Table of Contents

Business Email Compromise (BEC) fraud is arguably the most pervasive and persistent financial crime challenge facing U.S. business today. In fact, no less an authority than the FBI has identified it as the number one financial threat to U.S. business. The metrics back this up. In 2019, the FBI's Internet Crime Complaint Centre (IC3) recorded 23,775 complaints about BEC with losses of some $1.7 billion, an average of $71,500 per event. Furthermore, it estimated global losses over the previous three years in excess of $26 billion. **In a recent survey, the Association for Financial Professionals found that for six in 10 of all frauds investigated, BEC was the most common type of fraud members experienced.**

BEC Defined

The IC3 defines Business Email Compromise as a type of internet-based fraud that typically targets employees with access to company finances, using methods such as social engineering and computer intrusions. The objective of the fraud is to trick the employee into making a wire transfer to a bank account thought to belong to a trusted partner but that, in fact, is actually controlled by the fraudster.

That the fraudsters enjoy success in this activity is without question. That they also manage to achieve this with largely minimal interference from the authorities reflects the magnitude of the challenge.

There have been notable enforcement successes:

- 281 arrested worldwide in a coordinated international operation in 2019;
- A crackdown in the same year halting over 600 domestic money mules;
- An increase of 50 percent over the previous year;
- And the leader of a $120 million BEC fraud ring receiving a prison sentence in 2020.

But these successes pale somewhat when set against the metrics previously quoted, which is reinforced by Treasury Department reports of an average 1,100 businesses being scammed each month. How has BEC fraud reached this level of threat?

The Challenge

As real-time detection strategies have improved by using advanced analytic models, fraudsters have sought the path of least resistance in achieving their criminal aims. This path of least resistance involves using social engineering techniques to dupe individuals and more direct methods when duping businesses.

Take the case of the Lithuanian syndicate led by Evaldas Rimasauskas, for example. Beginning in 2013, his team regularly called the customer service centers of two U.S. target companies. Through this, they gained the names of key employees and relevant contact information. They also used phishing emails to gain access to the respective email systems of the two companies and gain further data of value. After two years of working through this process, the fraudsters were in a position to simply call each company pretending to be a vendor, have each change destination bank account numbers, and then have several payments wired totaling $120 million.

Rimasauskas was apprehended and convicted following a coordinated international effort, but if he had evaded capture, the potential return of $120 million from two companies over a two-year period would be deemed a somewhat stunning return on investment.

The Rimasauskas case highlights the key facets of a successful BEC criminal campaign. In the first instance, critical information is gathered about a company typically around key personnel and payment practices. This is achieved by social engineering of contact centers and reception staff. Even if staff received training in BEC awareness, fraudsters will simply find the weakest link and exploit it.

Secondary efforts center around phishing intrusions. Research indicates 135 million phishing attacks are attempted every day with the average cost of a U.S. data breach around $4 million. Given that people spend around 30 percent of their daily working life composing and answering email, then the statistical probability of success for the fraudster with this attack method is unfortunately relatively high. What can be done?

Ultimately, successful BEC fraud represents a failure to authenticate when accounting instructions are changed. Or more precisely, a failure to employ suitable analytic strategies to understand the nature of client payment instructions and employ suitable operational procedures to ensure payment risk is minimized. The following represents what NICE Actimize sees as a best practice in this area.

DEFINE - DETECT - DEFEND

NICE Actimize recommends combatting BEC fraud with three pillars of action – **Define - Detect - Defend**.

The first pillar is focused on understanding the client BEC challenge and in particular, the differing BEC fraud typologies faced.

Under the BEC heading we can encounter multiple sub-categories of fraud risk:

- BEC Business Email Compromise
- EAC Email Account Compromise
- VIS Vendor Impersonation
- FVS Fraudulent Vendor Scheme
- PCS Payroll Compromise Scheme
- ERS Expense Report Scam
- MCS Mortgage Closing Scam

By understanding risk at a more granular level, we are better able to differentiate fraudster modus operandi, which then allows for the development of more targeted analytics and profiling strategies coupled with supporting operational processes.

We first ***Define*** the problem and then we look to ***Detect*** the transactions that represent risk to the organization. The ***Detect*** pillar comprises the fraud strategies employed to alert on BEC transaction risk and includes using analytic models, behavioral profiling and user defined rules.

At the core of analytic models lies the predictive variables defined by the data scientist in association with the Fraud SME (Subject Matter Expert). In tandem with this, we have the behavioral profiling of expected customer payment patterns and corresponding vendor relationships together with the profiling of customer payment history so that normal transactions are understood and, more importantly, the provenance of those transactions.

Once these profiling statistics are collected and relationship data collated, real-time analytics needs to be deployed to detect and alert on risky transactions at an acceptable false-positive level. Fraudsters will continually shift their pattern of attack but as the Rimasauskas shows, their ultimate aim remains the same: to identify targets, gather information on internal processes and execute fraud. The **define – detect - defend** best practice serves to disrupt this attack pattern.

The final pillar, ***Defend***, represents the logical and necessary endpoint of ***Define*** and ***Detect***. Only an operational team that is trained and, more importantly, has confidence in the BEC mitigation strategy employed, will persevere with the client contact and ensure that their client understands the risk of a specific transaction. In fact, it is recommended that key clients are informed of new operational procedures that have been instituted as a result of the improved profiling and detection strategies employed.

A BEC Use Case

This use case discusses a leading U.S. bank that was looking to revamp its ACH BEC strategy, detection systems and operational practises. NICE Actimize consultants were initially engaged to assess the current situation and help chart a way forward in implementing a more effective BEC program. The challenges faced were a low fraud incidence environment, high losses per incident and no standard fraud modus operandi associated with the overall BEC fraud typology.

In the first instance, NICE Actimize consultants identified nuances within the overall BEC fraud umbrella that allowed for more effective strategies to be developed. In particular, the consulting team were able to identify different BEC fraud typologies and developed detailed classification scheme on each typology. Some

of these are well-known like CEO and Invoice Fraud while others are less well understood. But as per the old adage, to understand the enemy is to understand the path to success.

This more effective granular analysis then saw the identification and development of specific predictive features or variables that were particularly suited to the machine learning strategies employed by NICE Actimize Data Scientists.

With improved predictive variables, better detection models can be developed resulting in BEC alerts being created at a lower false positive.

More effective identification of the fraud typology then allowed for the design and implementation of more targeted operational practises such as second tier tagging. Improved tagging logically leads to better performance in supervised machine models.

This completed what could be seen as a virtuous circle where the enhanced operational practices provided better tagging outcomes which then flowed into higher performing analytic models which then reduced the aggregate BEC Fraud risk by eliminating sub-categories of this risk.

But the real test is the performance of the combined efforts across consulting, analytics and operations. NICE Actimize is pleased to report that the client detected and successfully stopped two major seven-figure BEC fraud attempts of the type that typically would have been successful.

In other words, in these two BEC fraud events, neither the client bank nor its customers experienced any losses when typically, there would have been a multi-million-dollar loss outcome to deal with. This represented an outstanding result for the NICE Actimize program. It is also worth noting that the fraud loss avoided represented a huge return on investment for the program.

Moving Forward

BEC fraud is one of the most pressing financial crime challenges facing U.S. business today. With annual losses in the billions of dollars and fraudster attempts becoming more sophisticated, the challenge is indeed both pressing and daunting.

Against this, NICE Actimize has fused a unique defense methodology based on Best Practice pillars of ***Define***, ***Detect*** and ***Defend***. In the use case outlined, consultants engaged with the client to develop a more granular understanding of the BEC fraud typologies faced and in doing so lay the basis for the development of a series of more predictive features for model development.

This led to the implementation of effective detection strategies based on advanced analytics which provided more effective and trusted risk alerts for execution by the client Operations team. The outcome was a very successful ***Defend*** phase to the program with millions saved for all parties.

The Actimize methodology and supporting analytics and infrastructure is available to all financial institutions in both the US and globally.

Learn more about NICE Actimize fraud solutions here.

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

info@niceactimize.com | www.niceactimize.com/blog | @nice_actimize | /company/actimize | NICEactimize

NICE · ACTIMIZE