Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 8, Issue 2 (July-Desember) 2023
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

Business Email Compromise (BEC) Fraud and How to Prevent it

✉Dwi Siska Susanti, Fitria Errinandini Subandi, Naila Failasufa, Wibi Anska Putri
Advisor SustaIN (Mitra Juang Mandiri), Indonesia

ARTICLE INFORMATION
Article History:
Received September 30, 2022
Revised Desember 7, 2022
Accepted December 1, 2023

DOI:
10.21532/apfjournal.v8i2.307

ABSTRACT
Cybercrime is on the rise both at the national and cross-border levels. The latest mode of cybercrime is fraud using Business Email Compromise (BEC). A qualitive analysis method with literature study is applied to discuss two key questions of this paper. First, how does the BEC scheme occur?. Second, how an organization/company can prevent/mitigate the risk of BEC fraud. This paper concludes that BEC can be executed in the form of phishing emails sent by perpetrators (both internal and external actors of the organization) to the target victim (organization's employees) in order to deceive and obtain financial gain. Various efforts can be made by an organization/ company to prevent the risk of BEC fraud, among others in the form of implementing a risk management system, implementing an information security management system, and increasing the organization's internal awareness.

Keyword: Business Email Compromise (BEC), Fraud, Fraud Prevention, Risk Management.

1. INTRODUCTION

Technological developments and advances have had a considerable impact on people's lives. In the era of globalization, people are increasingly dependent on technology that can provide convenience in carrying out various activities, especially in business activities. On the other hand, competitive attitude in doing business is an opportunity for irresponsible individuals or groups to commit fraud. Protection of access to technology and internet networks cannot guarantee complete security of ongoing business processes. Ability and concern are characteristics that must be strengthened by business people in order to minimize misuse of technology and internet networks.

Cybercrime is increasingly prevalent, both at the national and cross-border levels. Increasingly sophisticated technology and the internet is an opportunity that is exploited by cybercriminals to commit organized crimes in a very broad scope. As a form of crime modernization, cybercrime can be committed globally by more than 1 (one) actor in several jurisdictions with the target victim also being in another country. One of the most common modes of fraud currently occurring is

How to Cite:
Susanti, D., S., Subandi, F., E., Failasufa, N., Putri, W., A. (2023). Business Email Compromise (BEC) Fraud and How to Prevent It. *Asia Pacific Fraud Journal, 8*(2), 269-280. https://dx.doi.org/10.21532/apfjournal.v8i2.307.

✉Corresponding author :
Email: : dwisiska.sustain@gmail.com

the misuse of electronic mail (e-mail) by criminals in business processes, in which the perpetrators appear to represent a company, or better known as Business Email Compromise (BEC). According to FBI records, the number of crimes using the BEC scheme has increased in the last five years and caused a loss of USD 2.4 billion in 2021. The perpetrators of this crime come from not only external companies, but also internal company employees.

This research aims to enrich the study of Business Email Compromise (BEC) fraud and how to prevent this crime. This paper will discuss two main things. First, what is BEC and how does BEC scheme work? Second, how can an internal organization prevent or mitigate risks so that BEC fraud does not occur?.

2. METHODS

To answer these two topics, the method used in this paper is descriptive qualitative analysis using a literature study approach. Analysis is carried out on literature sources and case studies that are relevant to the subject matter.

3. RESULTS AND DISCUSSION

Business Email Compromise (BEC) Fraud

At the 10th United Nations (UN) Congress in Vienna Austria on 10-17 April 2000, the term cybercrime was divided into two categories. First, in a narrow sense, cybercrime is called computer crime. Second, in a broader sense, cybercrime is called computer-related crime.

> *"Cybercrime in narrow sense is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them."*

> *"Cybercrime as a broader sense is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network."*

Cyber-attacks are common in Indonesia. Based on data from the National Cyber and Crypto Agency (*Indonesia: Badan Siber dan Sandi Negara/BSSN*), there were more than 700 million attacks in 2022. The types of cyber-attacks found by BSSN are dominated by ransomware or malware attacks, phishing, and hacking of website content, all of which lead to data theft. One of the modes of fraud that often occurs today is the misuse of electronic mail (e-mail) by criminals in business processes, in which the perpetrators appear to represent a company, or better known as Business Email Compromise (BEC). The United States Federal Bureau of Investigation (FBI), on its official website, explains that BEC is a sophisticated fraud method targeting businesses and individuals who make legitimate fund transfer requests. When committing fraud, the perpetrator compromises a legitimate business or personal email account through social engineering or technical computer intrusion to make an unauthorized transfer of funds. From 2010 to 2022 in the last 2 (two) years, The Indonesian Financial Transaction Reports and Analysis Center or INTRAC (*Indonesia: Pusat Pelaporan dan Analisis Transaksi Keuangan / PPATK*) reported that the Crime of Money Laundering (TPPU) through the BEC mode has entered the financial system in Indonesia. Based on PPATK data, there are 437 accounts in Indonesia that are suspected of being intermediaries for money (money mules) resulting from cyber-crimes. 242 of these accounts were reported as suspicious financial transaction reports (LTKM).

In 2021, 4 (four) Indonesian citizens who had committed fraud through the BEC scheme were arrested by the Criminal Investigation Agency of Indonesian National Police (Bareskrim Polri). They deceived companies from South Korea (SI) and from Taiwan (WWHF) and made a profit of up to IDR 84.4 billion for their actions. The losses suffered by the victims are of concern to the wider community, so

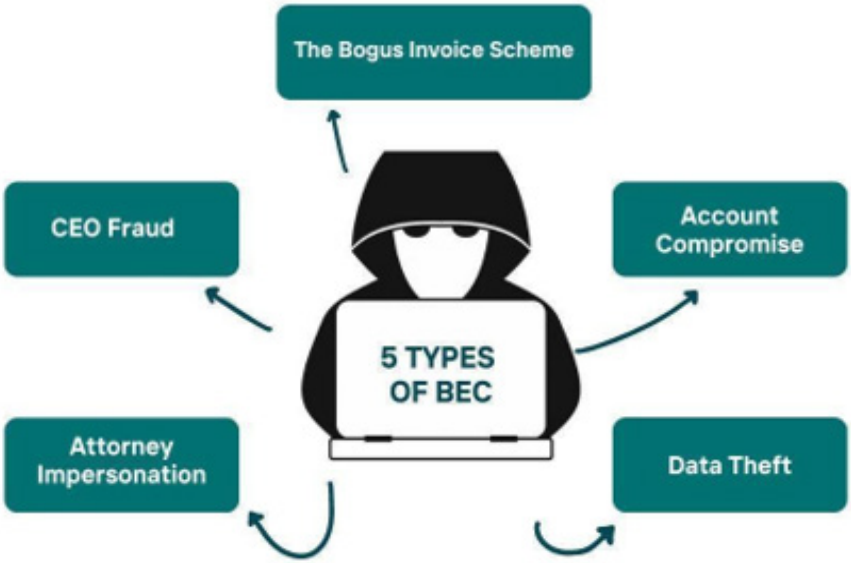
there is a need for initiatives or guidelines so that every company/organization is not trapped in this widespread and growing mode of crime. Based on the PPATK report, BEC cases that have occurred frequently must be immediately mitigated so that similar incidents will not occur again in the future. This case must be immediately handled not only by business actors which are companies, but also by the respective authorities such as PPATK and the Financial Services Authority (OJK). Every company needs to be more aware, recognize, and understand effective steps in mitigating the BEC fraud based on cases that have been successfully handled by Indonesia itself, other countries, or international organizations.

According to the FBI, BEC is a sophisticated scam targeting businesses that work with foreign suppliers and/ or businesses that regularly perform wire transfer methods (money transfer transactions between banks in other countries). BEC is part of the practice of spear phishing, in which fake emails are directed at company personnel in an attempt to obtain account numbers, access codes or other sensitive information. The most frequently used BEC modes are: (1) creating and using a fake email that is almost the same as the name of the company or the name of the executive/leader in the company (a trusted source) with the aim of tricking the victim; (2) attaching malware in emails sent to victims to hack networks and obtain sensitive information from target actors (spear phishing); (3) sending an attachment to an e-mail accompanied by company letterhead, in which the perpetrator gives an order to transfer an amount of funds to a trusted company business partner via an overseas bank. The FBI classifies BEC attacks into 5 (five) types, which can be seen in the following illustration.

a. *The Bogus Invoice Scheme*-the perpetrator uses fake invoices to deceive companies. In practice, this mode is commonly used when companies deal with foreign suppliers.

b. *Chief Executive Officer* (CEO) *Fraud* – in this mode, the perpetrator pretends to be a company executive to send emails to employees, usually in the finance department, and directs them to transfer an amount of money to an account that the perpetrator controls. As an example:

Figure 1. **Types of BEC Attack**



Source: Zweighaft, 2017

Table 1. **Example of Comparison of Original Email (Victim) and Fake Email (Perpetrator)**

Original Email (Legitimate)	Fake Email
nai_pit@abc.com	nai_pit@abc.co

Source : Data Processed

c. *Account compromise* – Account compromise-the perpetrator hacks executive or employee email accounts to use them illegally with the aim of requesting certain payments. The payment is sent to the bank account belonging to the BEC perpetrator.
d. *Attorney Impersonatio*n – Knowing that the company has attorneys who have responsibility for certain matters and company secrets, the perpetrator impersonates an attorney or someone from the law firm.
e. *Data Theft* – The perpetrator obtains personally identifiable information (PII) or employee and executive tax returns by targeting a company's resources or accounting department.

How does BEC fraud work?

ACFE states that fraud can be committed by various groups with inherent categories/ characteristics, such as:

a. The perpetrator who threatens individuals
   The perpetrator has a target to steal the personal identity of the victim of fraud by phishing in emails, and directs the victim to make an up-front payment transaction.
b. Fraud by/against the internal organization
   This happens when individuals or groups from internal organizations deceive their own organizations/ companies, such as embezzling, manipulating tax payments or reporting, and deceiving related vendors or business partners.
c. Fraud by/against external organizations
   This type of fraud can be perpetrated by vendors. For example, they ask for other costs separately to employees outside the existing agreement. Other examples are vendors sending counterfeit products or products that do not comply with applicable standards, sending checks with nominal values that have been intentionally changed (extra/decreased), or committing theft of intellectual property and customer information.

BEC mode can be done with the three fraud options above. Fraud perpetrators using the BEC mode can come from internal organizations and threaten the organization. Employees try to use various methods to conceal their actions, such as falsifying documents, recording misrepresented transactions, or abusing internal controls. In many cases, BEC perpetrators also join organized crime groups to share information in order to gain access to a company's email. Crime groups help BEC perpetrators find and buy stolen user's credentials to take over email accounts. Based on data obtained from the FBI (2021), The Internet Crime Complaint Center (IC3) received 19,954 complaints due to BEC with losses of up to USD 2.4 billion.

The BEC fraud has occurred since 2013. The modes most frequently used by BEC perpetrators are:

a. The perpetrator pretends to be a CEO and sends fake invoices with payment orders to employees of the organization/company. The invoice has been adjusted to the template that is usually used by the organization/ company;
b. The perpetrator sends an email to the victim as if there is an urgent payment and must be paid immediately. In this mode, the perpetrator has usually succeeded in hacking one of the employee's emails to trick the victim;
c. The perpetrator uses a fake name (usually using an employee's name) and attaches a phishing link that directs the victim to a website or application that is commonly used

by organizations/companies to make transfers/payments.

The Covid-19 pandemic has suddenly forced people's lives, including business activities, to adapt to remote and online activities. This has triggered an increase in the number of cybercrimes, including the potential for BEC to be used to commit fraud. In some cases, the perpetrator begins by sending an email containing a virtual meeting invitation to the victim using the BEC mode. Furthermore, the perpetrator used the virtual meeting to direct the victim to make a fictitious transfer to the perpetrator as if there was a bill for payment to the perpetrator as the vendor for the activity. To ensure their action, the perpetrators in the meeting also tricked the victim by inserting the deep fake of CEO without audio, or using fake audio.

The typical target for BEC is a company that has a high number of financial transactions - basically any company that transfers money on a regular basis. With adequate technological capabilities, perpetrators can easily hack confidential information from companies/ organizations that they will use to carry out transactions for profit. In several cases, both national and international, the BEC fraud case has a similar modus operandi to corporate fraud, by tricking the target company's personnel into sending a sum of money, which is generally of high value. After getting money from fraudulent transactions via e-mail (BEC), the perpetrators will send the money to other fake accounts that have been created based on confidential information that they managed to hack, and the money is usually sent to bank accounts abroad. After successfully receiving money abroad, the perpetrators withdrew the money and used it for their personal interests. This shows that the fraud mode of using BEC is also followed by money laundering to disguise the origin of the proceeds from BEC crimes. In fact, this happens by using cross-border financial transactions. Based on PPATK data (2021), BEC is one of the high-risk modes of money laundering for Indonesia.

In practice, BEC fraud perpetrators usually impersonate the victim's business partner with the aim of profiting from the victim's funds. In this case, the modus operandi of the perpetrator is as follows:

a. The perpetrator makes legality documents using fake identities (i.e. Trade Business License (SIUP), Systematically Important Bank (SIB), Location Permit, and Notary Deed);
b. The perpetrator forges the victim's company email address by changing/ reducing the characters in the email address. One example is the fraud against the WWHF company, where the perpetrator tricked the victim by falsifying e-mail address that was almost indistinguishable. Email forgery can be seen as follows (Table 2).

Table 2. **Example of Comparison of Original Email (Victim) and Fake Email (Perpetrator)**

Original Email	Fake Email
mmontufar@ naturipesfarms	mmontufar@ naturipefarms

Source : Data Processed

a. The perpetrator sends false information via email to trick the victim regarding changes in account numbers (the intended account belongs to the perpetrator);
b. Fraudulent funds are usually sent to another fake company's account, taken in cash, and exchanged for USD.

The Indonesian National Police (Polri) has achieved several successes in handling ML cases, one of which is the settlement of money laundering (ML) cases through the BEC mode which involved a Dutch company (MMS) as the victim. The two perpetrators who claimed to be one of the Korean companies (SD Bio) took action by sending false information via e-mail regarding changes in account numbers, so that payments for rapid test equipment entered the accounts of BEC perpetrators.

The fraud caused MMS to suffer losses reaching USD 3,597,875 (IDR 52 billion). The loss resulting from this case is IDR 276 billion.

Based on the two cases above, the Indonesian Law Enforcement Officers have carried out a series of fairly effective handling, such as following up cases through inter-agency collaboration (the Indonesian National Police and PPATK), and this evidence can be used in the judicial process so that the perpetrators are subject to criminal sanctions. The Indonesian National Police is coordinating with PPATK and related banks to postpone transactions on accounts in the name of fake company created by perpetrators. In addition, the National Police also succeeded in recovering assets owned by MMS of IDR 27 billion.

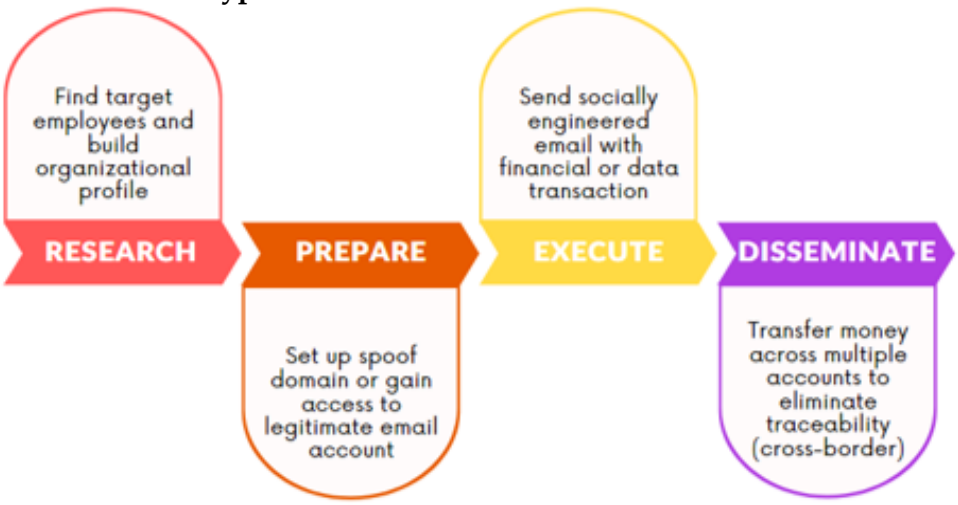
Not only in Indonesia, similar cases also occurred abroad, in 2019 the United States (US) Department of Justice (DOJ) in Virginia alleged three defendants in a money laundering case through the BEC mode. The perpetrators hacked into the victim's company's computer system, including its servers and email accounts. The perpetrators disguised themselves as business partners and claimed information that the business partners' bank accounts had changed. Due to the very convincing visualization of the email, the victim's company sends money to the fake accounts set up by the perpetrators. The defendants laundered more than USD 13 million which was obtained fraudulently from various business transactions of the victim's company. The perpetrators opened bank accounts that were used to make money transactions from or to domestic and foreign countries. One of the defendants, IB, spent USD 40,000 on luxury goods. In handling this case, each defendant was sentenced to a maximum of 20 years in prison. It is unavoidable that the perpetrators can come from within a company or organization. This can be proven through the case in Virginia above, one of the defendants was a banker who opened access to bank data so that it could be used by the perpetrators.

How to Prevent BEC Fraud

Based on FBI research in 2021, BEC is the most difficult mode of fraud to prevent or handle. Perpetrators can easily access all sensitive and confidential information data to be used as a way for them to communicate with the target/victim. There is an interesting fact that one of the reasons why BEC is still prevalent in various countries is that many businesses do not report these crimes to the relevant authorities to be followed up.

There are various efforts that can be made by companies/organizations to prevent the occurrence of BEC which

Figure 2. **How Does a Typical BEC Attack Work?**



Source: Armorblox, 2020

can be detrimental to the organization. **First**, companies/organizations can review security measures by examining information security in the internal environment including PCs/Computers, networks, and other communication devices; establish a system/framework that can detect unauthorized logins; and perform a step-by-step authentication process. **Second**, companies/organizations need to ensure confirmation with related parties such as communicating directly if there is an email regarding "Changes in Bank Information"; and answer emails by using the "Forward" function instead of "Reply". **Third,** the company/ organization needs to review the fund management framework by reviewing the fund management authority in situations when the authorized representative is not present and establishing an internal audit framework such as by affixing two signatures in each document to be approved.

Fraudsters with the BEC mode use various technical tricks and social engineering methods to gain trust and commit acts of fraud. Social engineering is a technique that takes advantage of individual (human) weaknesses to obtain information that is used to break through security systems. Social engineering attacks generally use direct interaction, either direct communication or online. It is during this interaction that the perpetrator uses social engineering techniques to influence the psychology of the victim.

Adequate understanding of psychological triggers can prevent perpetrators from committing social engineering crimes. Therefore, to mitigate the occurrence of BEC fraud, employees need to receive training in dealing with social engineering. The training/workshop provided will help employees/workers to be aware of and recognize BEC attacks.

The European Union Agency for Law Enforcement (Europol) provides efforts that can be made by companies/ organizations or employees as follows (Table 3).

In the early stages, BEC mitigation can be carried out by providing awareness training regarding what is meant by BEC, and how organizations/ companies can defend themselves from BEC attacks, including using the BEC detection application made by an internal organization/company. As part of prevention, organizations/companies also need to carry out two-step verification (multifactor authentication/MFA) of payment requests and invoices from vendors/suppliers if there are suspicious and unusual document attachments. In addition, organizations/companies need to create a culture of information security and tiered systems in the organizational/ company structure.

Efforts to strengthen the internal control system to prevent, detect, and respond to fraud with the BEC mode, especially in the digital era, are effective steps that can be implemented by internal organizations/companies. These efforts can be done in several steps as follows:

Implementation of Risk Management System

In preventing BEC attacks, companies/ organizations can implement risk management based on the International Standard Organization (ISO) 31000:2018 – Risk Management. There are 3 (three) main stages in the implementation of risk management: (1) Risk identification; (2) Risk analysis; and (3) Risk evaluation. To avoid fraud mode via BEC, companies/ organizations need to have a risk register that specifically looks at how high the risk of BEC is in ongoing business processes. From the results of the identification of these risks, companies/organizations can make plans to mitigate them, among others:

a. Companies or organizations shall understand and identify risks related to the BEC fraud mode. If there is an incoming e-mail from a company executive, vendor or business partner, it is necessary to re-identify it, especially in relation to e-mail accounts,

e-mail domains, data attached, and information/how the perpetrators communicate with the target/victim;

b. Leaders and management of companies/organizations are committed to providing training/socialization to all employees regarding the prevention of BEC fraud mode. This can be done by conducting periodic phishing test delivery trials so that they are more aware and find out how BEC mode can occur and how they can play an active role in preventing it;
c. Based on some existing data, the fake e-mail sent by the perpetrators attaches the amount of funds that must be transferred on behalf of the CEO of the organization/company, vendor or related business partner. To prevent organizations/companies from getting caught up in BEC fraud, organizations/companies need to make a contingency plan in terms of payments, for example by developing a protocol for payment approval, where there needs to be data validation and approval of certain employees (from the finance department) to identify whether the transaction is a fraud or not;
d. Emphasize all organizational/company personnel to maximize the use of the existing reporting system, including determining who is responsible for reporting BEC fraud to the relevant law enforcement authorities;
e. Establish a special team (preferably from the finance department) to coordinate with law enforcement authorities and related financial institutions, such as recipient banks, to freeze funds to prevent fraud and money laundering that may occur.

Implementation of Information Security Management System

Apart from ISO 31000:2018, there are other standards that can specifically be used as BEC mode mitigation efforts: ISO 27001:2013 – Information Security Management Systems. ISO 27001:2013 has 114 steps to control information security, which are then narrowed down. In its

Table 3. **Efforts to Mitigate the Risk of BEC Fraud That Can Be Carried Out by Companies/Organizations and Employees/Workers**

For Companies/Organizations	For Employees/Workers
Be aware of risks and ensure that employees/workers are informed about forms of fraud	Strictly implement security procedures that apply to payments and procurement, not skipping a step
Encourage employees/workers to process payment requests with care	Always check email addresses carefully when handling sensitive information such as making money transfers
Implement internal protocols regarding payments	If there is any doubt regarding the transfer order, consult a competent colleague
Implement procedures to verify the legitimacy of payment requests received via email	Do not open suspicious links or attachments received via email. Be careful when checking personal e-mail on company computers
Establish reporting routines to manage fraud	Limit information and exercise caution regarding social media
Review information posted on corporate/public institution websites, limit information, and exercise caution with regard to social media	Avoid information about company hierarchy, security, or procedures
Improve and update technical security	

Source : Data Processed

implementation, companies can choose which controls are most relevant to conditions in the field by conducting risk and asset assessments at an early stage.

Organizations or companies can mitigate information security risks by implementing several controls, among others:

a. The Organization/company need to identify risk owners, for example divisions that have business processes attached to information security systems. In its implementation, risk identification must refer to the loss of confidentiality, integrity, and availability of information within the scope of the information security management system.
b. The Organization/company shall determine the next action in the ongoing business process. In this case, the actions taken must include a continuous improvement plan and have a positive impact in order to achieve an adequate information security system. For example, providing training to employees whose duties and responsibilities are attached to digital transaction processes, so that they will be more aware of and understand the use of information systems owned by organizations/ companies, and they will find it easier to detect early potential BEC fraud.
c. The Organization/company need to establish policies related to information security systems that are published and documented to employees and relevant external parties.
d. The organization/company must separate conflicting duties and responsibilities to reduce the chance of unauthorized or accidental modification, for example related to the misuse of organizational/company assets.
e. The Organization/company need to establish policies to protect information that is accessed, processed, or stored in the information security system used.
f. The organization/company must conduct an employee background verification check in accordance with applicable regulations, and the verification must be proportional to the business requirements and the classification of information to be accessed.
g. The organization/company shall ensure that contractual agreements with employees and business partners/vendors state their and the organization's responsibilities for information security.
h. The organization/company shall ensure that all employees, and where relevant, business partners/vendors receive appropriate education and awareness raising training regarding information security systems.
i. The organization/company must identify information assets and classify them according to the level of protection required by the organization/company.
j. The organization/company must ensure that access and control policies are established, documented and reviewed based on the business process and information security system requirements.
k. The organization/company must provide and implement procedures for using a secure information security system, and ensure employee responsibility in using the system for authentication.
l. The Organization/company must establish security parameters to protect areas containing sensitive and critical information.
m. The Organization/company must ensure data protection and integrity, from backing up data, preventing malware, to maintaining internal logs.
n. The organization/company must maintain the security of the internal network and information leaving the organization.
o. The organization/company must analyze the impact of implementing an information security system.

p. The organization/company must test the information security system application to ensure that there is no adverse impact on the organization's operations or security.
q. The organization/company must establish information security requirements to reduce risks related to business partners' access to organizational assets.
r. The Organization/company must ensure that employees and business partners record and report any weaknesses in the information security system.
s. The organization/company shall establish, document, implement and maintain processes, procedures and controls to ensure the necessary requirements for an information security system in adverse situations.
t. The organization/company shall identify, document and update regulations and requirements for each information system.

Raising Awareness and Responding BEC

Organizations/companies need to ensure the concern of every member of the organization/company regarding the dangers of fraud with the BEC mode as one of the risks of the organization/company and ensure that they play an active role in preventing and reporting to the whistle blowing system and other complaint channels. In addition to detecting BEC, this can also be an effort by organizations/ companies to respond to BEC incidents carried out by/with the involvement of internal actors or by external actors of the organization/company. If BEC occurs and the organization/company or worker becomes a victim, apart from responding internally, the organization also needs to play an active role in reporting BEC crimes to law enforcement officials so that this case can be followed up with law enforcement processes (eradication efforts). To avoid fraud with the BEC, it is necessary to increase the capacity of law enforcement and establish cooperation among all relevant domestic and foreign stakeholders, for example by involving the role of the Indonesian Embassies in various countries, global financial intelligence networks, and interstate law enforcement coordination networks. Given the BEC mode is often done across countries.

From some of the explanations above, one of the good practices of implementing the ISO 27001 standard - Information Security System is the use of Amazon Web Services (AWS). AWS is a platform for storing organizational/company data from various sectors that already have an adequate information security system. AWS has also implemented the CIA Triad Security system which includes Confidentiality, Integrity and Availability. In the early stages, organizations/ companies that use AWS services in their business processes form a security baseline consisting of several indicators that need to be met.

a. Know your responsibilities
   AWS is responsible for the security of all of its user (client) data, for example in the use of applications, user identity, and most importantly the security of information systems within the overall organization/company environment.
b. Know your risk
   Organizations/companies need to carry out an assessment of potential information security risks, bearing in mind that AWS is a data storage service that is widely exposed to the internet.
c. Limited access through Identity and Access Management (IAM)"
   Provides limitations on the use of a system, where AWS service users can only be accessed by certain resources that are trusted by the organization/ company. It also aims to improve the integrity of the users who are granted such access.

4. CONCLUSION

Based on the description above, BEC is a type of fraud that can be committed by actors from internal and external organizations/companies. BEC uses

digital means by involving complex stages with the aim of tricking victims so that perpetrators can take advantage. BEC is included in cybercrime. In Indonesia, BEC is also a high-risk mode of money laundering.

Various efforts to prevent BEC can be carried out by internal organizations/ companies by (1) implementing a Risk Management System (ISO 31000:2018); (2) implementing an Information Security Management System (ISO 27001:2013); and (3) increasing awareness through optimizing the use of the whistle blowing system and reporting to law enforcement officials/relevant authorities.

REFERENCES

Aggarwal, V. (2022), *Why Business Email Compromise Still Tops ransomware for Total Losses*, https://www.csoonline.com/article/3670548/why-business-email-compromise-still-tops-ransomware-for-total-losses.html.

Andriyanto, T. (2022). Komunikasi Termediasi Penipuan dengan Modus Business Email Compromise (BEC), *Jurnal Riset Komunikasi (Jurkom), 5*(2), 220-243. 10.38194/jurkom.v5i2.627.

Armorblox. (2020). *What is Business Email Compromise? A Definitive Guide to BEC*. Cisco.

Asaf, Cidon, et.al, 2019, *High Precision Detection of Business Email Compromise. California: Proceedings of the 28th USENIX Security Symposium*.

Association of Certified Fraud Examiners (ACFE), *Fraud 101: What is Fraud*, fraud#:~:text=%E2%80%9CFraud%E2%80%9D%20is%20any%20activity%20that,%E2%80%9D%20(Black's%20Law%20Dictionary).

CNN. (2022). *RI Dihantam 700 Juta Serangan Siber di 2022, Pemerasan Dominan*. CNN Indonesia.

Cross, C. (2020). Exploiting Trust For Financial Gain: An Overview Of Business Email Compromise (BEC) Fraud. *Journal of Financial Crime, 27*(3), 871-884. 10.1108/JFC-02-2020-0026.

Dirgantara, A. (2021). *Penipu Perusahaan Asing Rp84,4M Lakukan Aksinya dengan Modus E-mail Bisnis*. Detik.com. https://news.detik.com/berita/d-5748751/penipu-perusahaan-asing-rp-848-m-lakukan-aksinya-dengan-modus-e-mail-bisnis.

Dokyung, Lee, et al, 2020, *A Study on the Effective Countermeasure of Business Email Compromise (BEC) Attack by AI*, Vol. 30, No. 5, Sep.

Dutcher, C. P. (2022). Pandemic Phishing: Business Email Compromise during Covid-19. *Dissertation*. Utica University, No: 29170430.

European Union Agency for Law Enforcement (Europol). (2019). CEO/*Business Email Compromise (BEC) Fraud*. https://www.europol.europa.eu/sites/default/files/documents/4_ceo-bec_fraud.pdf.

FBI. (2021). *Internet Crime Report*. Federal Bureau Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

FBI. (2022). *Business Email Compromise* (BEC). Federal Bureau Investigation. https://www.fbi.gov/file-repository/email-compromise_508.pdf.

Luxiana, K. M. (2020). *Penipuan dengan Modus Business Email Compromise terhadap Perusahaan Asing*. Detik.com.

MUFG Bank. (2022). *Don't be a Victim of BEC!*, https://www.mufg.co.id/images/editor/files/To_prevent_Business_E-mail_Compromise_ind.pdf.

Muncaster, P. (2021). *Banking Insider Accused of Role in $1m BEC Scheme*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/banking-insider-accused-role-bec/.

PECB. (2016). *Business Email Compromise (BEC): Don't Bite the Bait*. Professional Evaluation Board and Certification. www.pecb.com.

PECB. *(*2022*). Cybersecurity Risk Assessment*. Professional Evaluation Board and Certification. https://insights.pecb.com/tag/cybersecurity/page/2/.

PPATK. (2021). *Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang.* Pusat Pelaporan dan Analisis Transaksi Keuangan. https://www.ppatk.go.id/publikasi/read/150/penilaian-risiko-indonesia-terhadap-tindak-pidana-pencucian-uang-tahun-2021.html.

Remorin, L., Flores, R., Matsukawa, B. (2022). *Tracking Trends in Business Email Compromise (BEC) Schemes. Trend Micro Forward-Looking Threat Research (FTR) Team*ss. Trend Micro ™.

Rianto, A. (2000). *Metode Penelitian Sosial dan Hukum*. Granit.

Sean, A., Shahar. (2019), An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals. *Dissertation*. Doctor of Philosophy in Information Systems, College of Computing and Engineering, Nova Southeastern University.

Soekanto, S. (2006). *Pengantar Penelitian Hukum*. UI Press.

United Nations. (2000). *Crimes Related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network*. https://worldcat.org/title/4769476134.

Vinocur, J. (2022). *Death by a Thousand Paper Cuts: The Scourge That Is Business Email Compromise*. https://media.goldbergsegalla.com/wp-content/uploads/2022/04/22085043/Death-by-a-Thousand-Paper-Cuts_Vinocur.pdf.

Vorobeva, A., Khisaeva, G., Zakoldaev, D., Kotenko, I. (2022). *Detection of Business Email Compromise Attacks with Writing Style Analysis.* Springer. https://doi.org/10.1007/978-981-16-9576-6_18.

Winata. (2020). *Ratusan Rekening di RI Tampung Duit Kejahatan Siber Capai Rp 1T*. MEDCOM. https://www.medcom.id/nasional/hukum/8kolgXYK-ratusan-rekening-di-ri-tampung-duit-kejahatan-siber-capai-rp1-t.

Zulfahmi, M. (2022). Mencegah Serangan Rekayasa Sosial dengan *Human Firewall*, *Jurnal Sistem dan Teknologi Informasi, 10*(1).

Zweighaft, D. (2017). Business Email Compromise and Executive Impersonation: Are Financial Institutions Exposed?. *Journal of Investment Compliance, 18*(1), 1-7. 10.1108/JOIC-02-2017-0001.