



**Fraud Insights**

Selected COVID 19 - Related Fraud Schemes

July 2020

# How COVID-19 is affecting the overall level of fraud

Dear Sirs,

Coronavirus pandemic has affected our personal lives and will have a more significant impact in the future. Not only our relationships could change but whole perception on the economic world has transformed. Many companies discovered that home office can lower their costs and employees work more effectively... but also many companies found out that their employees have not much discipline.

Notwithstanding, working remotely, travel bans, an increased reliance on technology and economic uncertainty have become the reality for many businesses recently. Companies had to shift their focus on logistical and operational challenges to satisfy the needs of all stakeholders. However, these challenges are not the only ones faced. The crisis also opened the doors for increased pressure, opportunity and rationalization which can lead to fraud.

According to an Association of Certified Fraud Examiners' ("ACFE") survey conducted from late-April to mid-May 2020 amongst its members, as of May 2020, 68% of anti-fraud professionals had already experienced or observed an increase in fraud levels, with one-quarter saying the observed increase has been significant. Looking forward, anti-fraud professionals expect an even greater shift in the overall fraud levels. Nearly all of the survey respondents (93%) said they anticipate an increase in fraud in the next year (i.e., through to May 2021), with more than half of respondents predicting a significant increase. It seems that situation is evolving very fast and fraudsters continue to adapt. Given the many mitigating factors making fraud detection even more challenging than usual, it's essential that businesses are equipped with advanced solutions.

In this Newsletter we would like to inform you how the supply chain is affected, about the possible impact of Covid-19 on Financial Statement Fraud, what can be potentially dangerous for your employees in the terms of phishing and how organizations can protect themselves from such threats.

We wish you good reading.



**Impact of  
COVID-19 on  
financial  
statement fraud**

# Impact of COVID-19 on financial statement fraud

The COVID-19 pandemic has affected almost every country in the world and in turn it has **impacted almost every organisation**. Not only has it disrupted normal business operations and supply chains but it has also led to increased fraud risks for businesses and in particular the risk of financial statement fraud.

## According to ACFE surveys :



The primary risk factor in **22%** of all financial statement frauds is a poor tone at the top from senior management.



Employees are now working from home more, thus anti-fraud controls are now exposed to new unforeseen risks with an estimated **41%** increase in financial statement fraud which can be directly linked to Covid-19 expected in the coming 12 months.



Financial statement fraud is typically the most costly with a median loss of **878 376** euros.

## Revenue and Sales Manipulation

Organisations may manipulate the sales and revenue figures in an attempt to try and minimize the impact of the lockdowns on business performance.

## Concealing other types of fraud

COVID-19 contributes to more fraud by creating financial pressures and weakening internal controls (working remotely, staff reductions). Accounting records may be manipulated in order to hide losses incurred as a result of any type of fraud (theft, fraudulent transactions with related parties, other.) Thus, fraudulent financial reporting may be only the symptom of other frauds.

## Expense Capitalisation

Companies now have an increased incentive to capitalize expenses over extended and different accounting periods rather than expensing them in the appropriate period in an effort to minimize their expenses for the current financial period.

## Valuations and Impairments Manipulation Including Goodwill

As organisations face significant and unforeseen disruptions in business processes certain business assets both tangible and intangible may become impaired leading to misrepresentations of asset write downs.

## Disclosure Fraud

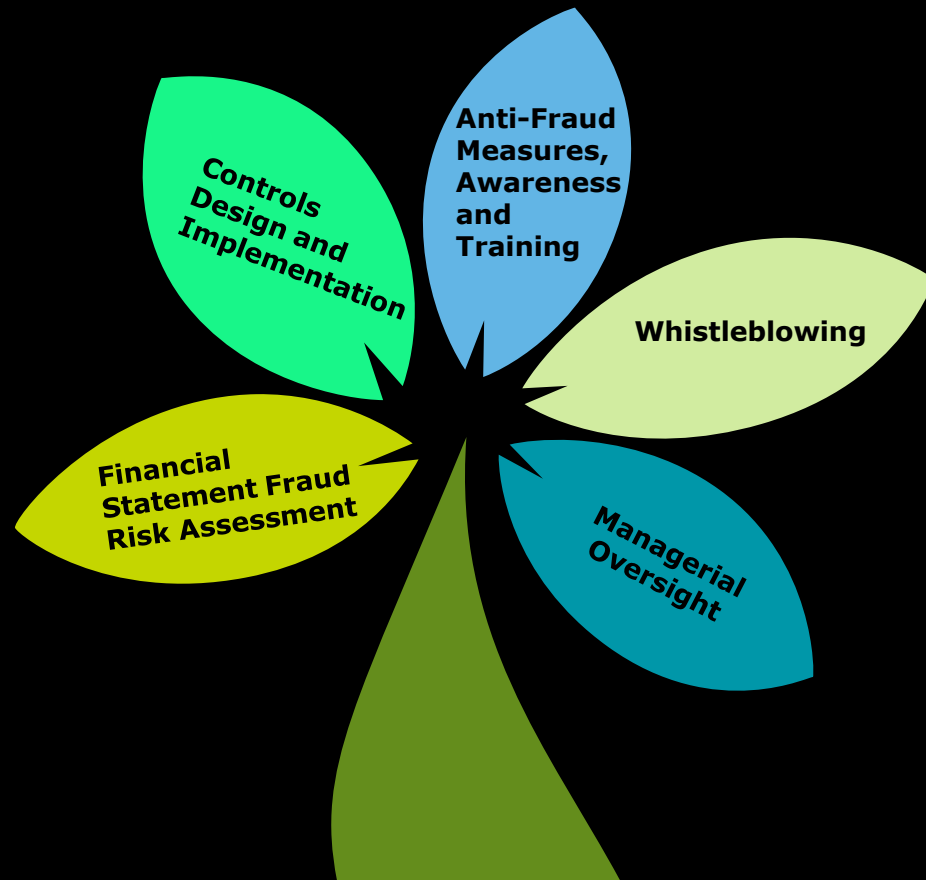
Organisations may be tempted to not fully disclose the overall impact of COVID-19 on the whole business in their financial statements to stakeholders.

## Going Concern and Liquidity

With sales revenues taking a sharp nose dive business have been forced to dip into their cash reserves in order to maintain business operations, pay staff salaries, and meet other financial obligations. This in turn created the risk that the going concern of the business will be severely impacted.



# How organisations can protect themselves from the identified risks



## Financial Statement Fraud Risk Assessment

Organisations need to revisit previously conducted financial statement fraud risk assessments in order to identify any changes, assess new levels of risk and make the necessary adjustments to the levels of fraud risk due to COVID-19's impact.

## Controls Design and Implementation

The focus on business operations coupled with vast numbers of staff working from home has left controls more vulnerable. Internal controls may be circumvented in times of crisis for the reason of expediency to keep business processes operating, but these are the same circumstances that fraudsters exploit. Thus organisations need to reassess the effectiveness of controls which are in place to mitigate fraud.

## Anti-Fraud Measures, Awareness and Training

Provide employees with tips on how to identify symptoms of fraud scams. This will in turn make them more alert in their daily work and will increase chances of early detection of potential fraud.

## Whistleblowing

Whistleblower notifications remain the key method of discovering fraud. Organizations may facilitate this process by providing tools for anonymous submission of notifications. Organizations should insure that all notifications are adequately analysed and investigated when this is warranted.

## Managerial Oversight

Management needs to stay ever vigilant and diligent by maintaining focus on internal and external audit and / or internal controls testing and strengthening activities to minimise loss and misconduct.





# Impact of COVID-19 on supply chains

# Supply chain impact of COVID-19

## Supply chain Disruption overview

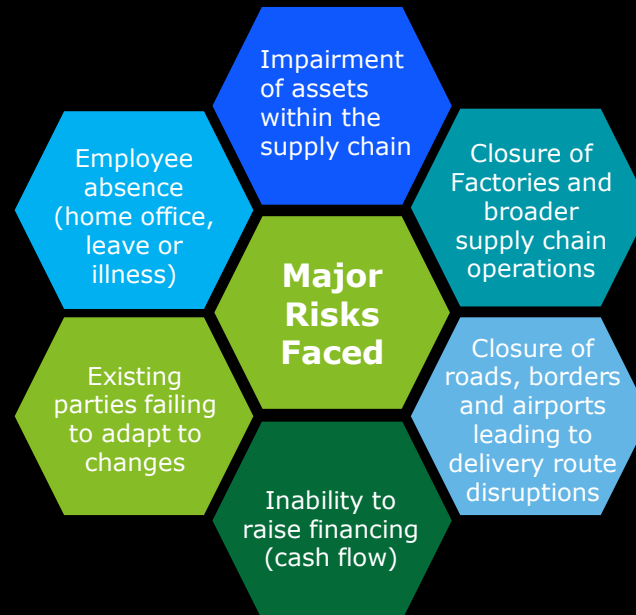
Organisations now find themselves having to adapt their already existing and established supply chains, logistics and manufacturing processes to the new restricted global business climate. This is an attempt to react timely to the changes and to effectively mitigate the impact of lockdowns and bankruptcies on their business processes.

Businesses need to take adequate, timely and effective measures to maintain business operations and continue to meet the demands of their customers and adequately support their employees.



In addition to supply chain disruptions, organisations also need to be cognisant of the impact on distribution and their retail partners. Stock piling of inventories, packaging and critical raw materials becomes important in maintaining the business operations of companies.

Furthermore the integration of many organisations in the CEE region into the open economies in Europe leaves them vulnerable to supply chain disruptions.



Large reductions for the second quarter of 2020 in Europe estimated to be at **7.8% or 12 million** full time workers.



**93%** of world population lives in countries with some form of travel or export restrictions.



Sectors most at risk include accommodation, food services, manufacturing, retail, business and administrative services.



In Poland total export of goods and services account for approximately **55%** of GDP.



The Polish Trade and Services Employers' Association observed among its members a turnover decrease of **45%** for Warsaw and **37%** for the rest of Poland in the first month after loosening of epidemic restrictions in comparison to the same period of previous year.

# Supply chain impact of COVID-19

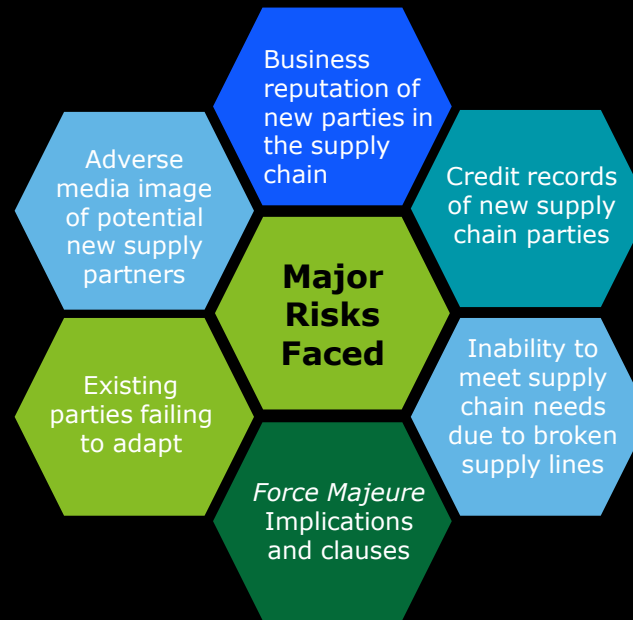
## Establishment of new supply chain relationships and supply chain mapping

With the imposed lockdowns across the world the delivery of goods by sea, air and freight has been heavily impacted and the supply of vital materials for businesses has been severely restricted.

This has in turn led a lot of business to start to seek local solutions to fill in the emergent gaps in their supply chains, thus a large number of affected organisations have established new business relationships with various local entities within a short period of time.

This has exposed organisations to various risks with the major risk being the establishment of business relationships without having properly vetted potential business partners and their capabilities.

While the safety of employees and clients is of the utmost importance during an emergency, companies must also ensure, to the extent possible, continuity of their operations. COVID-19 outbreak created need for social distancing, leading businesses to think about remote working solutions. Companies that used to interact with their customers face to face, are now starting to look at their businesses from different angles and search for ways to do things differently.



More than **312 Billion PLN** dedicated by Polish government to fight the crisis caused by Covid-19.



NBP cut interest rate by 40 basis points to **0.1%**.



The Federation of Polish Entrepreneurs estimates that between 16 March to 20 April alone Polish economy lost **79 billion PLN** due to restrictions on activity. 24 billion PLN of the losses are attributed to industry, 20 billion PLN to trade, 5 billion PLN to construction and 30 billion PLN to other service sectors.



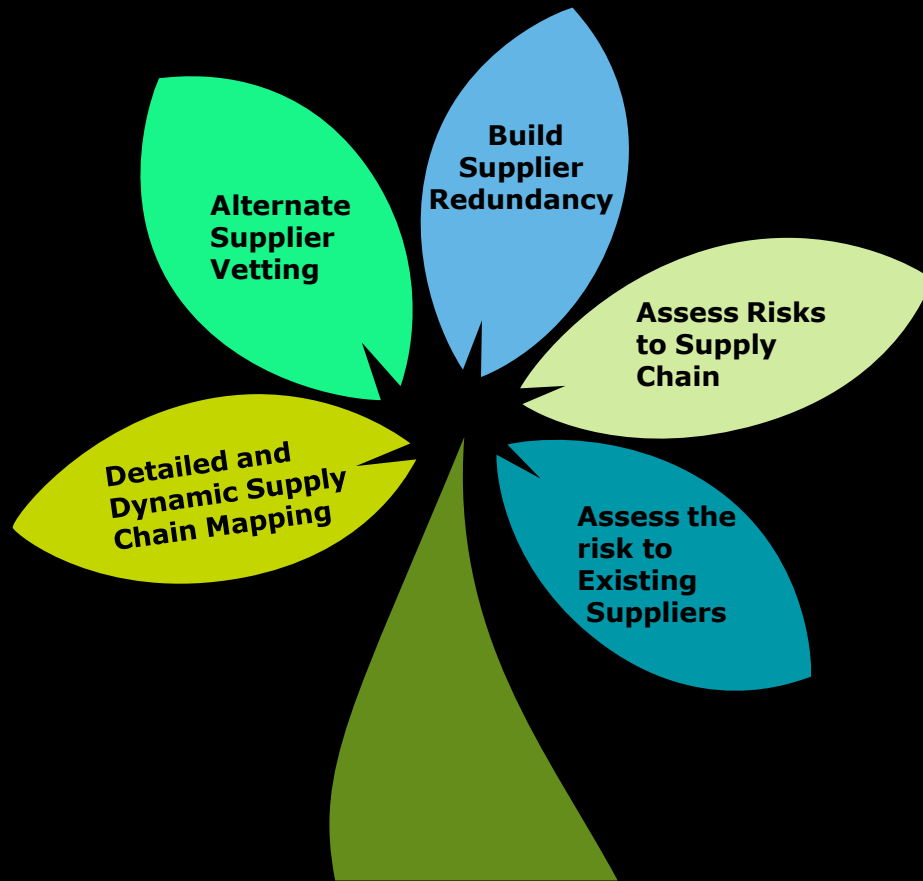
IMF expects the Eurozone's 19 countries to experience a **7.5%** contraction in their combined economies.



IMF expect Polish GDP to decrease by **4.6%** in 2020.



# How organisations can protect themselves from the identified risks



## **Detailed and Dynamic Supply Chain Mapping**

Assess how COVID-19 risks affects your Tier 1 and Tier 2 suppliers and develop a full picture of how your supply chain has changed and will change for both the long term and short term.

## **Alternate Supplier Vetting**

Identify potential alternate sources of materials for the organisation that are less affected by the restrictions and lockdowns. Vet all potential suppliers for their business and media reputation adequately to minimize the risk of entering into potentially detrimental business relationships for the organisation.

## **Build Supplier Redundancy**

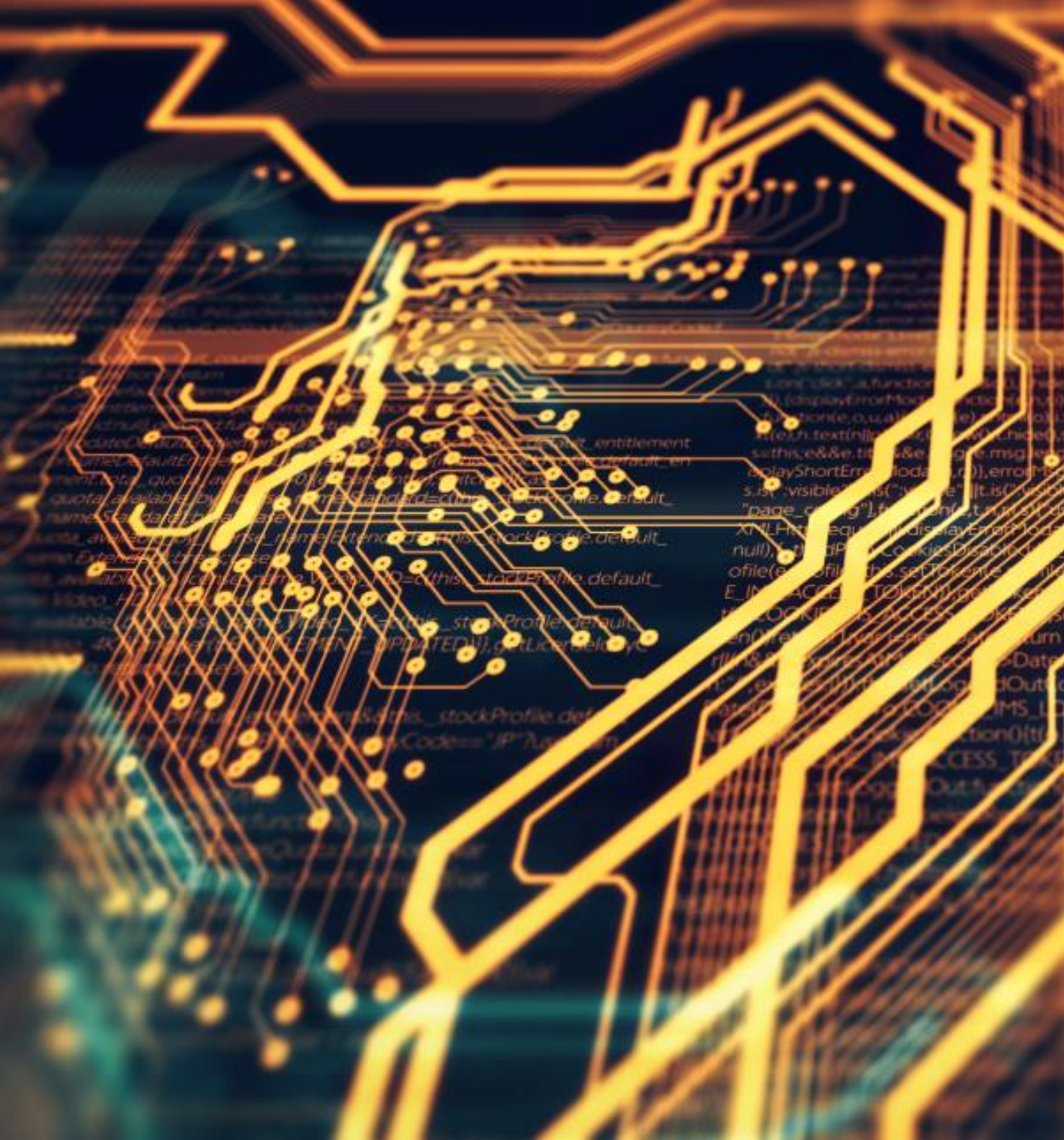
As part of the long term disaster mitigation and risk mitigation steps organisations should attempt to build redundancies within their supply chains so as to minimize the risk of broken supply chains affecting business processes.

## **Assess Risks to Supply Chain**

Organisations should develop a process (risks based) that identifies and assesses the emergent risks to their supply chain. All identified risks should be continuously monitored and the impact of any changes of the risks to the supply chain should be assessed promptly.

## **Assess the risk to Existing Suppliers**

The risk resulting from lockdowns should be assessed for the direct suppliers as well as for suppliers further down in the supply chain (supplier's suppliers).



# Impact of COVID-19 on Phishing

# Phishing

Managers **agreed** on **cutting** down **salaries** during crisis... For more information click here. **Your HR.**

## Reminder, what is **phishing**? Phishing during **COVID-19**


Phishing is a type of fraud where a victim who is impetuous or careless unknowingly discloses sensitive personal/company information and then fraudster misuses the information afterwards. The most often used form of phishing is committed via e-mails or SMS (smishing), but telephone channels work as well (vishing).

Why is the fraud called phishing? Because the fraudster tosses a "fishing rod" and just waits until some fish get caught.

The crisis mode makes it easier for fraudsters to target employees by sending "urgent" emails pretending to be from members of senior management, leading to employees disclosing sensitive information or wiring money.

Within a month of the initial China outbreak, cybersecurity companies began reporting email phishing scams related to COVID-19.

 **100 000 000** phishing e-mails blocked by Google **every day**

 **20%** of those emails were related to COVID-19 hoaxes\*

\*13-17 April 2020

A well-known Czech antivirus company has warned of the increased activity of fraudulent e-mails and sites that try to convince users to buy protective equipment, virus testers, or donate money to certain organisations. None of this is real and after the victim clicks on a button which redirects to a webpage where he/she fills out personal information, the fraudsters misuse this data.

The perpetrator takes advantage of the lack of attention of the victims, so for example he may simply swap two letters in the email domain or omit a letter. An example of this could be a domain "@gmal.com". Would you react on email deloittece@gmal.com?

There is also abuse of publicly known names, especially the WHO ("World Health Organization"), which is added to the email address. This can then take the form of who.alerts@global.org

Fraudsters can also abuse your company's business domain. For example, they will impersonate the HR department or the management of company which wants to report across the company about wages and bonuses during a pandemic. They can also impersonate your supervisor, who urgently needs to find out something from the attached file. The file will be named "COVID19\_threats\_for\_companies.pdf.exe", which, when overlooked, can evoke a pdf file with information. However, after opening, you unknowingly install a Trojan horse. Some users have hidden final file extensions, so only the "pdf" extension will be visible.



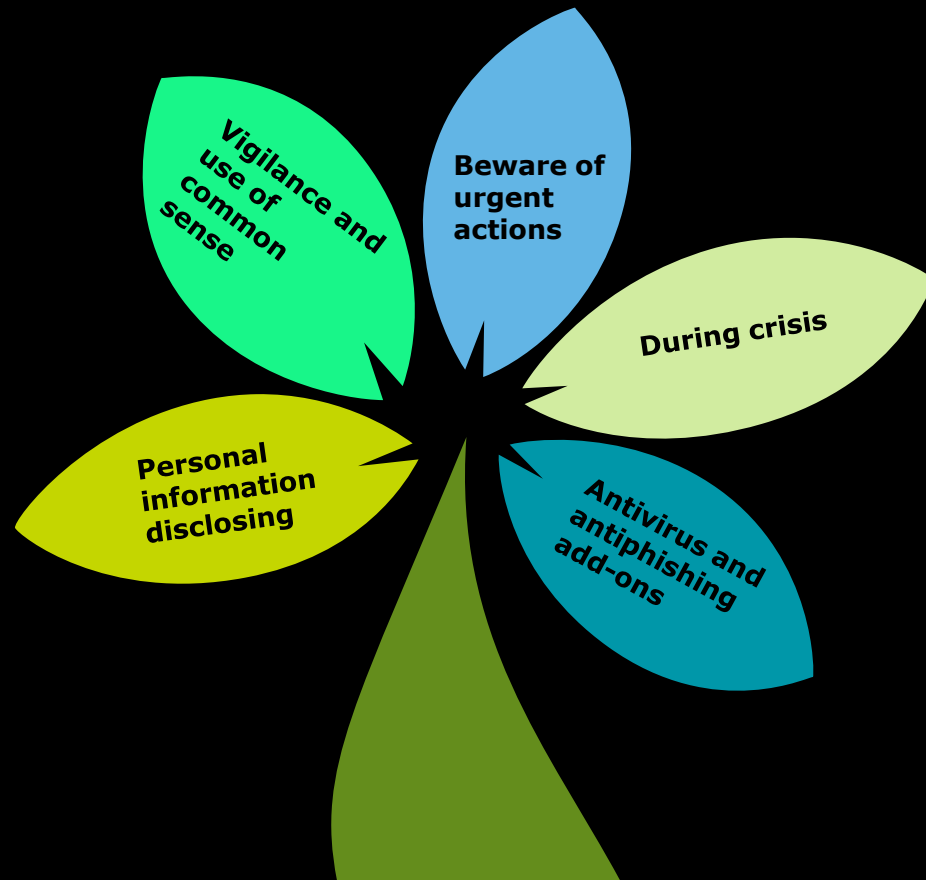
**...in any case, keep calm and delete the email!**

In order to increase employee awareness to the threat of phishing, a simulated phishing email can be sent to employees followed by training elements for employees who fail to identify the email as a phishing attempt.

But be careful! Using this technique carelessly can constitute a breach of law!



# How organisations can protect themselves from the identified risks



## **Be vigilant and use common sense**

Use common sense to spot suspicious emails. Always check an email address for misspelling and do not click on suspicious links open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device. If you want to learn about the link, you can always use Google or go directly to the company's website. Phishing emails will have impersonal greetings like „Hi dear” because they are meant for general audience.

## **Do not disclose personal information**

This is the general rule of the internet. You should not disclose personal or financial information via email. Go to the webpage of the company which demands this data and verify their activity and contact details. You can call them or come in person.

## **Avoid urgent actions**

Fraudsters will try to catch you by requesting immediate action e.g. requesting you to click on something or filling out a questionnaire with limited time. It might resend a renewal of insurance policy from your insurance company or donation to help fight the crisis. Typically, this leads to data harvesting sites. Again, think of the situation and remember to thoroughly scrutinize all urgent email requests!

## **During crisis**

Beware of fake funding organizations or e-shops selling necessary goods (facemasks, disinfection...). Always check the website, hot-line and reviews for particular company as well as delivery fees etc. Fraudsters try to use the fear and emotions arising from crisis and scare individuals into making purchases.

## **Have your antivirus updated**

Make sure the anti-malware and anti-virus software on your computer is operating and up to date. Antivirus companies are sitting on the knowledge of cyberattacks. Did you know you can install anti-phishing add-on to your browser?





Contact us if you have questions about the issues covered in this newsletter or other questions in the field of prevention, detection and investigation of unethical and fraudulent activities in organizations:

**Aaron Goldfinch**

Partner | Forensic Poland

Deloitte Advisory sp. z o.o. sp. k.

Al. Jana Pawła II 22, 00-133 Warszawa

Mobile: +48 662 155 399

agoldfinch@deloittece.com | www.deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services.

Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 312,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com)

Deloitte Central Europe is a regional organization of entities organized under the umbrella of Deloitte Central Europe Holdings Limited, the member firm in Central Europe of Deloitte Touche Tohmatsu Limited. Services are provided by the subsidiaries and affiliates of, and firms associated with Deloitte Central Europe Holdings Limited, which are separate and independent legal entities. The subsidiaries and affiliates of, and firms associated with Deloitte Central Europe Holdings Limited are among the region’s leading professional services firms, providing services through nearly 7,000 people in 44 offices in 18 countries.

© 2020. For information, contact Deloitte Poland.