

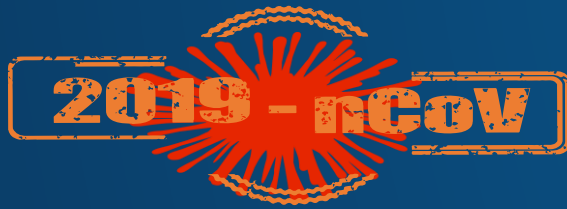


**2020 NATIONAL
CONFERENCE**
Indonesia Virtual Event | 2-3 December 2020



EMERGING TOP FRAUD RISKS TO CONSIDER IN 2021 AS A RESULT OF GLOBAL

**COVID-19
PANDEMIC**



IMPACTS TO INDONESIA

The World Health Organization declared the COVID-19 virus outbreak as a global pandemic on March 11, 2020. The virus has had unexpected human and economic consequences across many countries.

President Joko Widodo confirmed the first two cases of COVID-19 in Indonesia on March 2, 2020.

As of 31 October, Indonesia has reported 410,088 cases, the highest in Southeast Asia !!!

1 PEMBATASAN SOSIAL BERSKALA BESAR (PSBB)

Lockdown, social distancing and implementation of strong regulation of work from home (WFH) & school from home (SFH) policies. This has caused a lot of businesses to limit their operations and closed down.

2 UNEMPLOYMENT RATE

During the economic downturn caused by the coronavirus pandemic, the unemployment rate in Indonesia surged to **7.07 percent** in the third quarter 2020 compared to 5.28 percent in the same quarter a year earlier. The number of unemployed persons surged by 2.67 million to **9.77 million**¹.

3 GROSS DOMESTIC PRODUCT (“GDP”)

Badan Pusat Statistik (“BPS”)¹ announced Indonesia’s GDP growth fall **3.49 percent** (y-o-y) in the third quarter 2020, following a fall of **5.32 percent** (y-o-y) in the second quarter compared to the same period in 2019. Whilst the GDP only grew at 2.97% in the first quarter 2020, a sharp decline compared to the same quarter in 2019 which was 5.02%. **This has pushed Indonesia into its first recession in 22 years!**

EMERGING AREAS OF TOP FRAUD RISKS

Consideration for Audit Strategy 2021

The emergence of the COVID-19 pandemic has a devastating impact for many organizations globally. The combination of financial and health threats has exposed organizations to a variety of other emerging risks related to virtual operations, cybersecurity, changes on how we manage customers and suppliers that put pressure on the operations and also service delivery.

1

CYBERCRIME & DATA BREACHES

2

INTERNAL FRAUD: PEOPLE & BEHAVIOUR

(1) Corruption, (2) Asset Misappropriation, and
(3) Financial Statement Fraud

EMERGING AREAS OF TOP FRAUD RISKS

Consideration for Audit Strategy 2021

1

CYBERCRIME & DATA BREACHES

IN 2017, THE GLOBAL ECONOMY LOST \$600 BILLION AS A RESULT OF CYBERCRIME. CYBER ATTACKS GO FAR BEYOND FINANCIAL LOSS AND CAN IMPACT BUSINESSES' FINANCES, REPUTATION, OPERATIONS, AND STAFFS' MORALE.

1 CYBERCRIME & DATA BREACHES

73.7%

Penetration of internet users in Indonesia has reached 196.7 million people, 73.7% of total population of Indonesia in 2nd Quarter 2020, according to a survey from the Indonesian Internet Service Providers Association (APJII) ².

Indonesia is a country with the fourth largest internet users in the world after China, India and the United States ³.



Data BSSN⁵

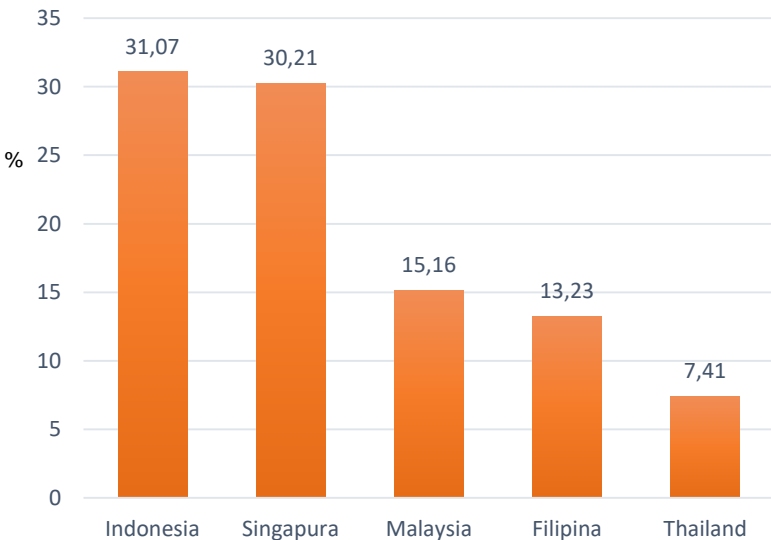
Badan Siber dan Sandi Negara (“BSSN”) recorded nearly **190 million cyberattack attempts** from January to August 2020, **almost FIVE TIMES higher** compared to the same period in 2019, around 39 million. The highest increased was in August 2020, where BSSN recorded around 63 million cyber attacks, much higher than in August 2019 which was only around 5 million.⁴

1

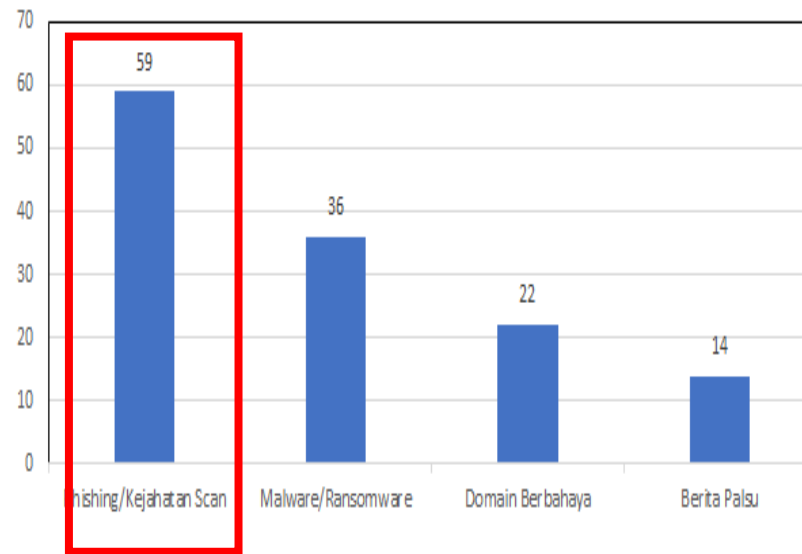
CYBERCRIME & DATA BREACHES

According to a 2020 report by the International Criminal Police Organization (Interpol), Southeast Asia has been targeted by cyber criminals who operate by tricking victims, or through phishing. **Indonesia is the main target for fraud perpetrators.**

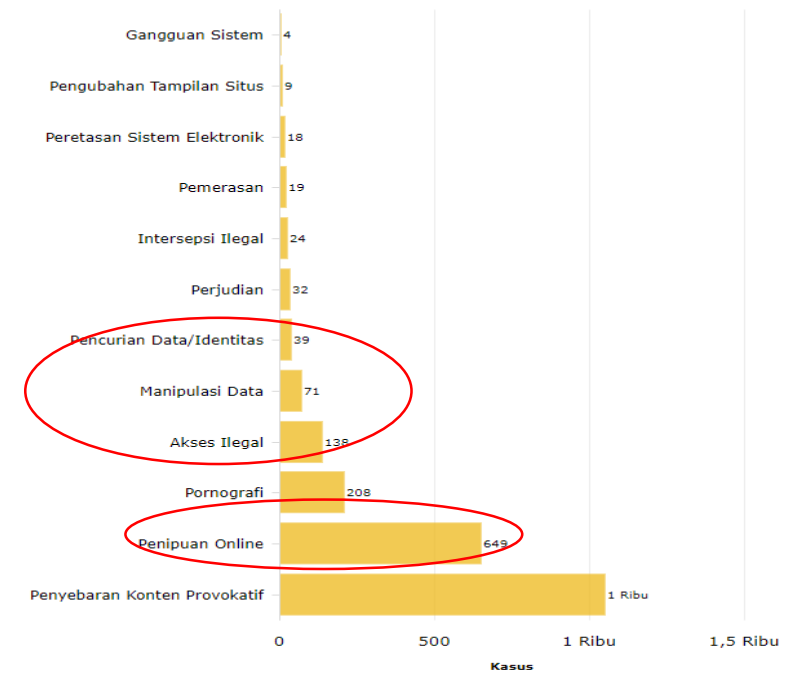
Tren Phishing di ASEAN Selama Semester 1 2019
(The International Criminal Police Organization⁶ 2020)



Serangan Siber Terkait Covid-19 Secara Global (Interpol, Agustus 2020)⁶



Laporan Kasus Kejahatan Siber Indonesia (Januari-September 2020)⁶



Sumber : Kepolisian Republik Indonesia (Polri)

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

ONLINE FRAUD (28.7%) is one of the most widely reported crimes occurred from January until September 2020.

1 CYBERCRIME & DATA BREACHES

CYBER ATTACKS RELATED TO COVID-19

80% Firms have seen an increase in cyber attack this year. Coronavirus is alone blamed for **238%** rise in cyber attacks on banks. Phishing attacks have seen a dramatic increase of **600%** since the end of February.

81 Global firms from **81** countries reported data breaches in the first half of 2020 alone.

Ransomware attacks rose **148%** in March and the average ransomware payment rose by **33%** to **\$111,605** as compared to Q4 2019.

(Source: Fintech News)

Software AG Ransomware Attack

The second-largest software vendor in Germany and the seventh-largest in Europe, Software AG has been reportedly hit by a ransomware attack in October 2020. ZDNet reported that the German tech firm has been attacked by the Clop ransomware and the cyber-criminal gang has demanded **more than \$20 million ransom**.

The report also says that the company has still not recovered from the attack completely. The company disclosed that the ransomware attack disrupted a part of its internal network. But services to its customers, including cloud-based services, remained unaffected. The company also tried to negotiate with the attackers but it all went in vain.

As per the statement released by Software AG, the company is in the process of restoring its system and database for resuming orderly operation.

Hack of Aussie Hedge Fund Using A Fake Zoom Invite⁷

A fake Zoom invite has led to the demise of a successful Sydney-based hedge fund and **nearly cost it \$8.7million** after a hacker was able to send off fake invoices on behalf of the firm.

On Monday, the AFR reported that Levitas Capital was forced to close after its major client Australian Catholic Super withdrew its funds in the wake of the September cyber attack.

The hedge fund's cyber investigators have pinpointed a fake Zoom invite opened by one of the fund's cofounders Michael Fagan or Michael Brookes.

By doing so, the hacker was able to install a malicious software program that gave them access to the fund's email system which they used to send off fake invoices.

2020 has been a challenging year for personal data protection with a series of data leakage cases, both experienced by the government and private companies.

230 THOUSAND OF COVID-19 PATIENTS

May 20, 2020: Covid-19 patients' data (name, citizenship status, date of birth, age, telephone number, home address) was suspected to have been stolen and sold on the dark web forum RapidForums.

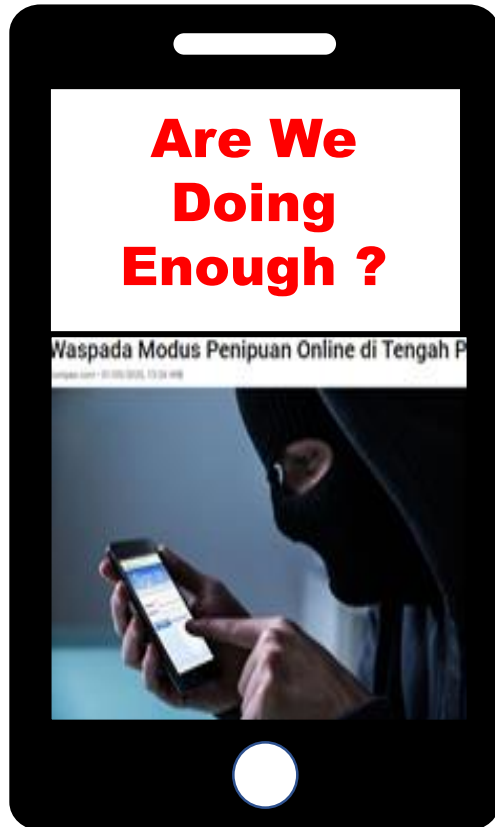
1.2 MILLION OF BHINNEKA.COM

May 11, 2020: A group of ShinyHunters hackers claimed that they had 1.2 million Bhinneka.com user data. They managed to break into Bhinneka user data and sold a total of 73 million user data from various other sites on dark web.

91 MILLION OF TOKOPEDIA ACCOUNTS

The perpetrator sold the data on the darkweb in the form of user ID, email, full name, date of birth, gender, mobile number and password which is still hashed or encrypted. They were sold at a price of USD 5,000 or around IDR 74 million.

Companies which did not have significant remote working capabilities are forced to invest quickly in acquiring and implementing technology. Inevitably such rapid roll-outs are likely to be less robust than infrastructure changes planned and tested over a longer period.



- ✓ Are employees fully aware of the phishing attempts which can result in malware / ransomware attacks?
 - ✓ How have the company's IT Security monitoring capabilities been disrupted over the last 12 months? What controls have been taken to mitigate such disruption?
 - ✓ Do employees understand the parameter of IT security? Are all devices being used with connectivity and network access secure?
 - ✓ Is there any password management system that allows distribution of credentials without putting the company's security at risk?
 - ✓ How has the WFH impacted the IT controls system in different parts of the business and what risks does this pose?
 - ✓ How has the new segregation of duties impacted the user access matrix in terms of roles and responsibilities?
- ✓ Has the business performed a risk assessment to identify possible network weaknesses and data assets that are vulnerable to cyberattacks and theft?
 - ✓ Is there a dedicated firewall management that is configured correctly to minimize this risk?
 - ✓ Are the anti-virus and anti-spyware software being installed and regularly updated to all computers including personal device?
 - ✓ Have new software applications (e.g. video conferencing software) adopted been adequately checked for potential security flaws and vulnerabilities?
 - ✓ Are employees trained to follow best practices, aware of the importance of data security and avoid mistakes that could lead to data breaches?
 - ✓ Are security patches on personal devices being updated and managed to the same standard with the organization devices?

EMERGING AREAS OF TOP FRAUD RISKS

Consideration for Audit Strategy 2021

2

INTERNAL FRAUD: PEOPLE & BEHAVIOUR

(1) Corruption, (2) Asset Misappropriation, and
(3) Financial Statement Fraud

IF YOUR ORGANIZATION IS FOUND TO BE ENGAGED IN FRAUDULENT ACTIVITIES, IT MIGHT NOT ONLY BE FACING FINANCIAL LOSS, BUT LEGAL LAWSUITS, DECLINE OF MARKET CONFIDENCE, PENALTY FROM REGULATOR, AND UP TO BUSINESS CLOSURE.

2 INTERNAL FRAUD: PEOPLE & BEHAVIOUR

FRAUD TRIANGLES



OPPORTUNITY

- Recognizing fake revenues or expenses
- Steal or distribute sensitive data when working remotely
- Forged or signatures on documents
- Setting of laptops / systems for WFH may result in users being given inappropriate system access
- Employee surveillance, whistle-blowing channels and internal investigation may not be operating at full capacity during WFH

RATIONALIZATION

- Rationalize the circumstances of no salary increase, bonus and pay cut during the year
- Perceived as if they borrow the money during this recession which will be payback later
- Inclined to commit fraud if WFH make employees feel disengaged or undervalued

PRESSURE

- Unsecured of jobs security / sustainability
- Individual performance tension to report positive results / meeting business target
- Significant new financial pressures on businesses which may lead to enhanced risk-taking or internal fraud

80.5%

The Association of Certified Fraud Examiners (“ACFE”) in 2009 shows that fraud is uncovered 80.5% more often in economic downturns than in stable times. The ACFE’s new 2020 fraud report shows that the average loss per fraud case is now \$1.5 million, most were being carried out internally.

2 INTERNAL FRAUD: PEOPLE & BEHAVIOUR

Companies need to shore up their detection and monitoring when fraud becomes part of the crisis

Top 5 types of fraud

1 Customer fraud

2 Cybercrime

3 Accounting fraud

4 Asset misappropriation

5 Bribery & corruption

Only 69% of US organizations use corporate controls to detect frauds

35% don't regularly test or audit their controls

10% have no normal fraud program in place at all

Source: PwC Global economic crime and fraud survey 2020 (US edition)

Examples of Fraud Red Flags During a Pandemic*

1 CORRUPTION

- ✓ Questionable use of third-party agents, consultants, or sales intermediaries who interact with government officials
- ✓ Insider trading
- ✓ Bribing to obtain or retain new business (or funding from government programs)

2 ASSET MISAPPROPRIATION

- ✓ Larceny of inventory
- ✓ Frequency of purchases and amount of vendor spend sharply increasing
- ✓ Volume of purchases not supported by a rational need
- ✓ Lack of physical control over assets
- ✓ Overstating or creating fictitious expenditures
- ✓ Falsifying hours leading to overstatement of compensation

3 FINANCIAL STATEMENT FRAUD

- ✓ Sales exactly meet budget or expectations
- ✓ Bonuses tied to sales
- ✓ Excessive returns after period-end
- ✓ Customer invoices show extended payment terms or unusual return allowances
- ✓ Improper inventory and other asset valuations
- ✓ Unapproved changes to vendor master file are unauthorized
- ✓ Pressure to manipulate financial estimates
- ✓ Write-downs to cover account shortfalls
- ✓ Data manipulation to breach financial covenants

*Source: A Blueprint to Managing Corporate Fraud Risk During A Pandemic, Nelson Luis, FLAI

2 INTERNAL FRAUD: PEOPLE & BEHAVIOUR

NEWS HEADLINES!

Berita Video

VIDEO: Gelapkan 6000 Material OVP, 3 Karyawan PT Ericsson dan 2 Penadah Diamankan Polisi

Senin, 2 Maret 2020 17:04



Ungkap kasus pencurian dan penggelapan material OVP yang melibatkan karyawan PT Ericsson di Mapolda Metro Jaya, Senin (2/3/2020).

lihat foto

f

t

wh


in

+

Selain Maybank, Ini Kasus Pembobolan Dana Nasabah Bank Sepanjang 2020

Berdasarkan data yang dihimpun *Bisnis*, setidaknya ada empat kasus pembobolan dana nasabah bank sepanjang tahun ini.

M. Richard - *Bisnis.com*
20 November 2020 / 13:44 WIB



Ilustrasi kejahatan siber - *NewsFoto/Rizki Permana*

Bisnis.com, JAKARTA - Baru-baru ini kasus pembobolan dana nasabah di perbankan kembali mencuat.

Berdasarkan data yang dihimpun *Bisnis*, setidaknya ada empat kasus pembobolan dana nasabah bank sepanjang tahun ini.

Tidak hanya alasan kejahatan siber, tetapi kasus ini juga terjadi karena oknum internal perusahaan.

detikNews > Berita

Survei TII: 82% Perusahaan Swasta Ngaku Rugi Akibat Suap

Lisye Sri Rahayu - *detikNews*
Rabu, 03 Jul 2019 17:08 WIB

3 komentar

SHARE f t



Ada Kasus Rekayasa Laporan Keuangan Jiwasraya, IAPI Sarankan Ini

Reporter: Caesar Akbar
Editor: Dewi Rina Cahyani
Senin, 13 Januari 2020 20:51 WIB

0 KOMENTAR

f t wh +





- ✓ Are the established controls for preventing and recognizing fraudulent behaviors available and working?
- ✓ Do the highest ethical standards continuously be promoted from top down in the organization? Is senior management walk the talk?
- ✓ Are your employees able to perform their BAU remotely? Is digital signature being used? Can employee review and approve the processes without encountering physical constraints?
- ✓ How has the new segregation of duties impacted the user access matrix in terms of roles and responsibilities?
- ✓ Has management taken a sufficient risk-based approach to the way business operates in response to the pandemic? Has this risk being assessed and documented? Any measures for the organization's risk appetite?
- ✓ To what extent does the organization's efforts to remain operational impacted its compliance risk? Have staffs been taking shortcuts that pose possible conduct and other regulatory breaches?
- ✓ Are there any controls in place to prevent theft of data by employees working remotely?
- ✓ Does your organization carry out a reprioritization of the risks? Are key controls in place to mitigate them?
- ✓ Do you send any risk reminder communications to staff of zero tolerance to fraud still applies and that employees should report any suspicious behavior or fraud?
- ✓ How is the organization's ability to manage fraud? Any whistle blowing being implemented in the organization?
- ✓ Has the monitoring and follow-up of suspicious transactions changed in any way? Is full monitoring capacity available during this time?

EMERGING AREAS OF TOP FRAUD RISKS

Consideration for Audit Strategy 2021

*Thank
you*

EMERGING AREAS OF TOP FRAUD RISKS

Consideration for Audit Strategy 2021

Sources & References

1. Badan Pusat Statistik, “Berita Resmi Statistik”, dated 5 November 2020
2. “Pengguna Internet Indonesia Mendekati Angka 200 Juta”, Kompas.com, Penulis: Wahyunanda Kusuma Pertiwi, Editor: Oik Yusuf
3. Internet Top 20 Countries – Internet Users 2020, <https://www.internetworldstats.com/top20.htm>
4. “BSSN Sebut Keamanan Siber RI 2020 Naik, Serangan Meningkat, CNN Indonesia, 27 September 2020, M. Ikhsan
5. “Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi”, Kompas.com, 12 Oktober 2020, Penulis: Putri Zakia Salsabila
6. “Kenali Maraknya Penipuan Online Saat Pandemi”, katadata.co.id, 7 Oktober 2020, Cindy Mutia Annur
7. “A Hacker Nearly Stole \$8 Million From An Aussie Hedge Fund Using A Fake Zoom Invite”, Gizmodo, 23 November 2020, Cam Wilson

END OF REPORT