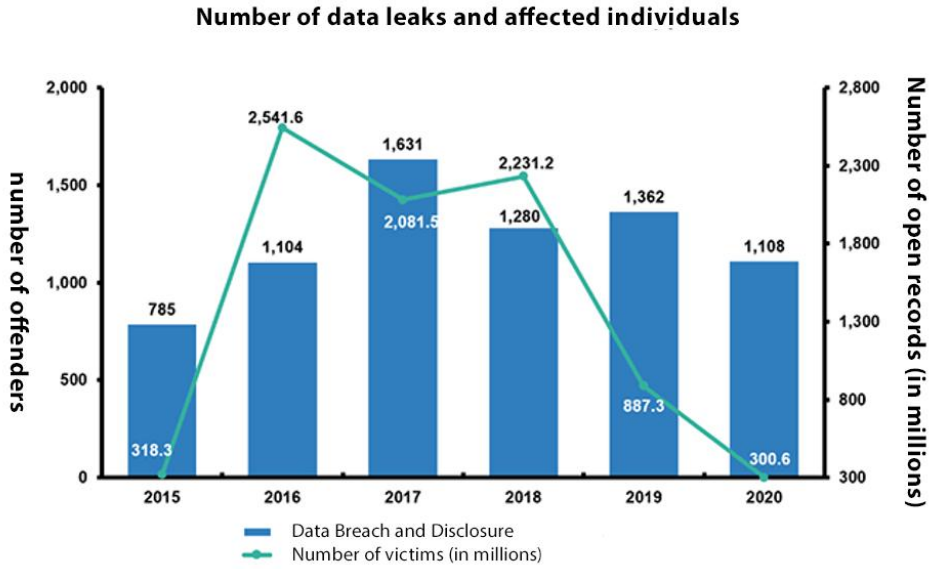
УДК 004

Дробот Т.С., студентка гр. 125-20-1
Науковий керівник: Олішевський І.Г., асистент кафедри БІТ
(Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна)

SELLING PERSONAL DATA

According to 2018 data, 63% of corporate data breaches are the sale of data from employees of those same companies. Employees do this for a variety of reasons, from a thirst to earn money for leaking databases to a competitor to trivial mistakes and negligence.

International security companies have summarized the statistics from 2015 to 2020 for data breaches and those affected, the chart below.



Based on this information, we can understand that most of it fell in 2016 and 2018. But these days, it hasn't come down to zero.

Let's break down the importance of data leaks.

No matter what the reason for the data leak, there will be a devastating blow to the company's reputation afterwards, a huge loss of revenue, and a danger to users, as their data can now be used for self-serving and fraudulent purposes.

This is a hot topic at the moment as the Philippine National Bureau of Investigation (NBI) recently reported on April 19, 2022 that a former Smartmatik employee involved in an alleged IT security incident on its network was promised a reward of up to 300,000 pesos (about US$6000) in exchange for access to his laptop which was connected to the company systems.

On 14 January, Smartmatik was contacted via email by hackers from the unknown group XSOS. They said they had infiltrated the network and stolen internal documentation. In the same email the hackers offered the company some "preventive services" but were turned down. A couple of days later, XSOS members sent another letter threatening to expose the stolen information to Congress and the media.

XSOS created four Facebook groups (on 19 January, 23 March, 26 March and 15 April) and uploaded photos of files allegedly taken from Smartmatic systems.

For its part, Smartmatik has taken a "stricter approach" to vetting employees and now requires them to leave their laptops in the offices. And 720 cases of illegal access have been filed against the employee. (source gmanetwork)

In that case, how can companies make sure that employees do not sell sensitive data? How can firms protect themselves? First, it's important to understand what data is being leaked, which employees are doing it and what their ultimate goal is:

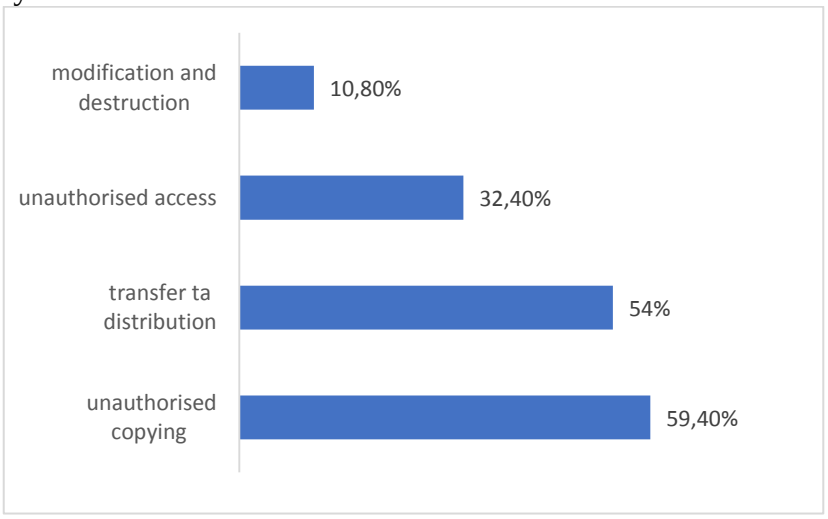
✓ 48% of staff tampering with corporate data stores occurred less than a month before termination.

✓ About 80% of rank-and-file attackers stole their employers' information for personal or competitors' gain, while privileged users were more likely to commit breaches for reasons other than money.

✓ In 54% of cases, confidential information stolen was either shared with third parties (including competitors) or made public.

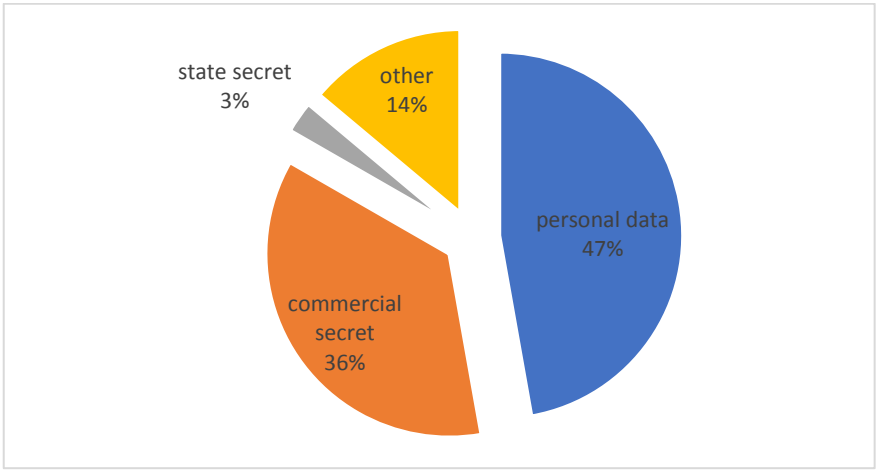
✓ In 57% of incidents, the stolen data was transmitted online, and 19% of leaks were via email.

The most common way employees make unauthorised copies of company data. Often cybersecurity incidents involve multiple disruptive actions, such as unauthorised copying of sensitive data (59%) and transfer of data to employer competitors, criminal gangs or others (54%). Unauthorised data access and data modification/destruction account for one in three and one in ten incidents respectively.

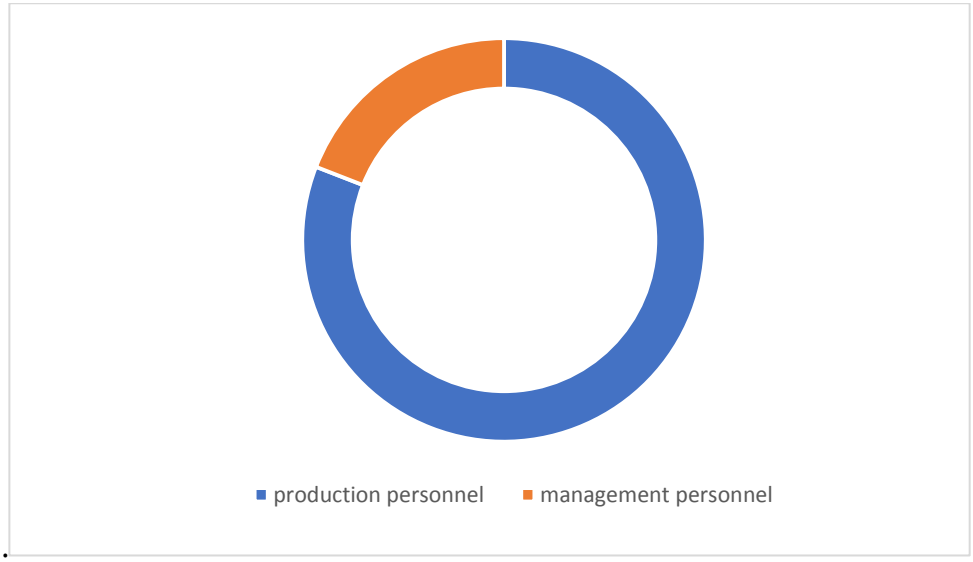


Destructive actions with data by employees

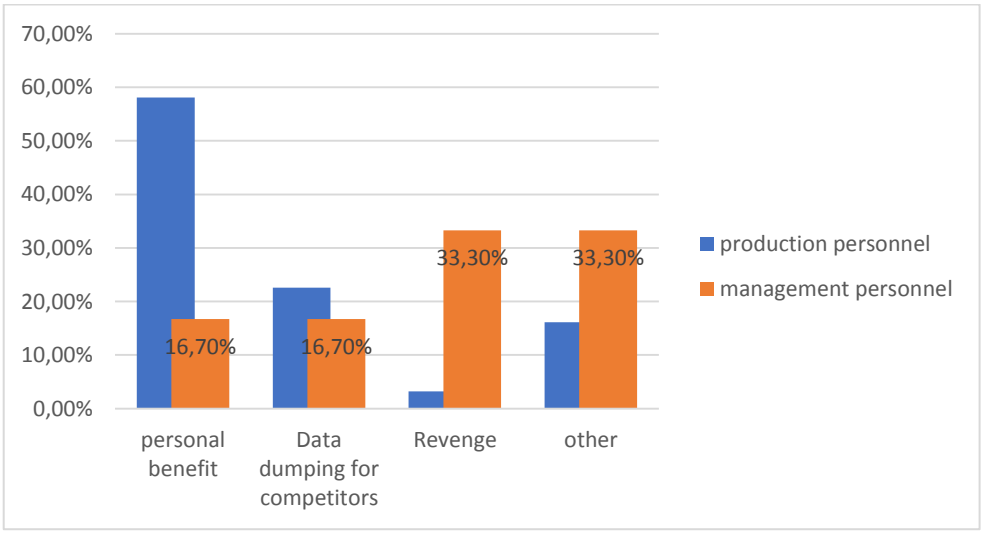
Statistically, almost half of all employees have taken or viewed databases containing personal information of their colleagues, customers or partners of their employer, and over a third of all employees have misappropriated commercial secrets



Types of data compromised by employees



Production personnel were behind 80.9% of all incidents reviewed, while management personnel committed about 19.1% of all violations



Types of perpetrators and reasons for the crime

So, with this information we now have an idea of how to prevent data leaks from company employees.

- Capture screenshots and video from screenshots, webcam images, audio from microphone and speakers (from work devices)
- Scanning of incoming and outgoing e-mails, attached files (from work devices)
- monitoring of communications in messengers Skype, Teams, Viber, Telegram, WhatsApp, etc. (from work devices)
- monitoring of visited websites and Internet requests, file transfers via file exchanges, web mail and chats (from work devices)
- Application usage statistics and text input monitoring
- Face recognition from webcams for presence monitoring and employee identification
- Work only on company devices, not employee personal devices
- removal of work devices outside of working hours

Data leakage in the corporate environment cannot lend itself to IT analysis because the important factor in this situation is the human factor, the communication of rank-and-file employees and management personnel, the relationships between company members, the level of access to important information by different levels of employees and the company's security

model. Existing methods do not take such subjective factors into account and therefore cannot predict destructive actions by employees.

Despite this, modern solution (monitoring) methods are already emerging that can help companies accurately predict employee behaviour thanks to evolving predictive analytics based on artificial intelligence, big data and machine learning.

This is exactly what will help reduce a company's risks in data leakage. Compliance with security measures is the result of a successful and prosperous company!

References:

1. Kim, K.; Kim, J. A Study on analyzing risk scenarios about vulnerabilities of security monitoring system: Focused on information leakage by insider. In Proceedings of the International Workshop on Information Security Applications, 2018.
2. Managing Digital Marketing in 2020 Research Report, 2019.
3. Insider Threat Report. Insider threat report. Insider threat related data breach detection time. 2019.
4. Accenture and HfS Research. The State of Cybersecurity and Digital Trust 2016.
5. https://www.gmanetwork.com/news/topstories/nation/829003/nbi-ex-smartmatic-employee-admits-money-offer-in-data-leak-mess/story/