From January 2019 to April 2020

Information leakage

ENISA Threat Landscape
A data breach occurs when data, for which an organisation is responsible, is subject to a security incident resulting in a breach of confidentiality, availability or integrity.¹ A data breach frequently causes an information leakage, which is one of the major cyber threats, covering a wide variety of compromised information from personal identifiable information (PII), financial data stored in IT infrastructures to personal health information (PHI) kept in healthcare providers’ repositories.

When security breaches are encountered in the headlines of bulletins, blogs, newspapers, and technical reports, the focus is mostly either on adversaries or on the catastrophic failure of the cyber-defence processes and techniques. Nevertheless, the undisputable truth is that, despite the impact or scope of such an event, the breach is usually caused by an individual’s action or by an organisational process failure.²
Findings

2,013 confirmed data disclosures in 2019
During the first half of 2019, the organisations experienced an 11% increase in disclosures compared with 2018.6

14% of all incidents in the financial sector were data disclosures
In 47% of them, the victim was a bank.9

4,1 billion data records were exposed globally in the first half of 2019
E-mail and passwords were at the top of the list.10

€5,46 million is the highest cost incurred by healthcare sector11
Kill chain

Information leakage

Reconnaissance  Weaponisation  Delivery  Exploitation

Step of Attack Workflow
Width of Purpose
The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.
Incidents

Top data leak incidents

- In January 2019, the independent researcher Troy Hunt found 773 million users' e-mail addresses and passwords in the cloud-storage service MEGA. Hunt named this breached dataset as ‘Collection#1’ and notified the service ‘Have I been Pwned?’ so it could notify the account owners to change their login passwords for accessing MEGA platform. In the same month, rogue individuals released personal details, private communications, and financial information of hundreds of German politicians, with targets representing every political party but the far-right AfD (Alternative für Deutschland).

- In February 2019, more than 61 million accounts were culled from 16 websites and put up for sale on the dark web. Site owners of Whitepages, Dubsmash, Armor Games, 500px and ShareThis saw their users' stolen data sold for less than US $20,000 (ca. €17,000) in Bitcoin.

- In March 2019, hundreds of millions of Facebook and Instagram users saw that their credentials were exposed by the social media company's poor password storage management.

- In April 2019, 12.5 million medical records of pregnant women were exposed in India, because of a leaky government server belonging to a healthcare agency. The medical information exposed was related to the pre-conception and pre-natal diagnostic techniques act, an Indian law passed which that banning pre-natal sex determination in an attempt to prevent Indian families from aborting unborn girls and skewing the sex ratio towards boys.
In May 2019, DoorDash, a food delivery service, suffered a data breach that affected almost 5 million users. The subsequent investigation determined that information such as names, e-mail addresses, delivery addresses, order history, phone numbers and passwords had been accessed. The company said that the last four digits of some consumers' credit cards and bank account numbers had also been accessed.\textsuperscript{16}

In June 2019, the American Medical Collection Agency (AMCA) began notifying clients of a system hack that breached the billing and medical data of some of its clients, including 11.9 million records of Quest Diagnostics, which is one of the largest blood testing companies in the United States. According to a recent Securities and Exchange Commission 8K filing, a hacker had gained access to the AMCA's system for nearly eight months between 1 August 2018 and March 30 2019.\textsuperscript{17}

![Information disclosure root causes. Source: Ponemon, IBM Security\textsuperscript{22}](chart.png)
Top data leak incidents

- In July 2019, the financial corporation Capital One suffered an information leakage that affected 100 million credit card applications, 140,000 social security numbers and 80,000 bank account numbers. Capital One reported that no credit card account numbers or login credentials were exposed. However, the breach exposed names, addresses, postal codes, phone numbers, e-mail addresses and birth dates.\(^{18}\)

- In August 2019, 160 million records of MoviePass were left unencrypted. Because the company's database wasn't password-protected, it left customers' credit card numbers and other details exposed. The database remained online for several days.\(^{19}\) Meanwhile, a massive leak exposed 27.8 million biometric staff records held by the British Metropolitan Police, banks and defence contractors. The database was administered by Suprema, a company that collaborates with the British police.\(^{20,21}\)

- In September 2019, more than 218 million ‘Words with Friends’ player accounts were hacked. The users' database included data from Android and iOS players who had installed the game before September 2. The hacker team ‘Gnostic players’ accessed information such as players' names, e-mail addresses, login identities and more.\(^{22}\)

- In October 2019, Adobe left 7,5 million Creative Cloud customer records on an insecure database. The information leakage included the users’ e-mail addresses and payment status.\(^{24}\)

- In November 2019, Facebook gave inappropriate access to the profile data of its 70,000 customers to about 100 app developers. One of them stole the personal data and later used these data to scam them.\(^{25}\)
In December 2019, a Dutch politician faced 3 years in prison for hacking 100 women’s iCloud accounts and leaking nude pictures. The politician was found to have hacked the women's personal iCloud accounts with credentials found in earlier public database breaches. During the same month, the details of over 10.7 million Metro-Goldwyn-Mayer (MGM) resort guests were disclosed on a hacking forum. The leaked information included full customer name, home addresses, phone numbers, e-mail addresses, and birth dates.

Breach incident rates by level of security spent. Source: CNET

<table>
<thead>
<tr>
<th>Security is more than 10% of the IT budget</th>
<th>Security is 10% or less of the IT budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ever</td>
<td>Within past year</td>
</tr>
<tr>
<td>40%</td>
<td>19%</td>
</tr>
<tr>
<td>52%</td>
<td>29%</td>
</tr>
</tbody>
</table>

Breach incident rates by level of security spent. Source: CNET
The primary attack vector in information leakage is insiders. This term is used to describe a person with an interest in ‘exfiltrating’ important inside information on behalf of a third party. Other common attack vectors used by this threat are misconfigurations, vulnerabilities and human errors.

How

Types of sensitive or regulated data stored. Source: Thales⁴⁸
“A data breach frequently causes an information leakage, which is one of the major cyber threats, covering a wide variety of compromised information”

in ETL 2020
Proposed actions

- Anonymise, pseudonymise, minimise and cipher data in accordance with the provisions of the EU GDPR, the California Consumer Privacy Act (CCPA), and the China’s Multi-level Protection of Information Security (MLPS 2.0). Always check the regulation commitments for counterpart entities who do not fall under bi- or multi-lateral initiatives.

- Store data only on secure IT assets.

- Limit user access privileges under the need-to-know principle. Revoke access privileges of anyone who is not an employee.

- Educate and train your organisation’s personnel periodically.

- Use technology tools to avoid possible data leakages, such as vulnerability scans, malware scans and data loss prevention (DLP) tools. Deploy data and portable system and device encryption, and secure gateways.

- A business continuity plan (BCP) is crucial for dealing with a data breach. This plan outlines the type of data being stored and their location, and what potential liabilities could arise when implementing data security and recovery actions. A BCP entails an effective incident response, which aims to address, manage, and rectify the damages caused by such an incident.
“In many cases, companies or organisations are not aware of a data breach happening in their environment because of the sophistication of the attack and sometimes the lack of visibility and classification in their information system.”

_in ETL 2020_
References


ENISA Threat Landscape Report
The year in review
A summary on the cybersecurity trends for the period between January 2019 and April 2020.

ENISA Threat Landscape Report
List of Top 15 Threats
ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

ENISA Threat Landscape Report
Research topics
Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.
ENISA Threat Landscape Report

**Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

**Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

**Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.
The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union’s infrastructure, and, ultimately, to keep Europe’s society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and all members of the ENISA CTI Stakeholders Group: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact
For queries on this paper, please use enisa.threat.information@enisa.europa.eu. For media enquiries about this paper, please use press@enisa.europa.eu.
Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Cybersecurity (ENISA), 2020
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Wedia. For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu