INFOWATCH®

DATA BREACH REPORT 2018

A STUDY OF DATA LEAKS IN THE MIDDLE EAST

TABLE OF CONTENTS

Table of contents 2

Report findings 3

Conclusion and findings 9

Leakage monitoring on the InfoWatch website 10

Glossary 11

REPORT FINDINGS

InfoWatch Analytics Center has released a report on personal data, payment details and other confidential information leaks in the Middle East (Bahrain, Jordan, Israel, Yemen, Qatar, Kuwait, Lebanon, UAE, Oman, Saudi Arabia, Syria), as well as geographically and culturally close Iraq and Iran, and Northern and North-Eastern Africa (Algeria, Egypt, Libya, Morocco, Sudan, and Tunisia) – all of which will be hereinafter together referred to as the “Middle East”.

The report is based on publicly available cases, with the sampling being sufficient to compare it with the global data leakage landscape. The authors analyzed information security incidents that clearly involved data compromising, selecting approximately 60 data breaches from businesses, public organizations, and governmental agencies in the Middle East over the period from July 1, 2017, to June 30, 2018. While the global sample for the same period included 2,000+ data leaks, both reports employed the unified list of metrics, thus making the research findings comparable.

The authors believe that both global and the Middle East surveys cover a maximum of 1% of all assumed leaks due to the extremely concealed nature of incidents involving data compromising. However, InfoWatch selected leak classification criteria in such a way so that each category group contained sufficient or excessive number of items (actual data leaks). This approach to survey fielding allows having theoretical sample, with the findings and trends identified in the sample being representative for the aggregate total.

The InfoWatch analysts believe that the research allowed them to describe the big picture of the data breaches in the region and compare key breakdowns of global and regional leaks. This report is a valuable source of basic information for business owners, top managers, CISOs, cybersecurity system developers, and generally all those who take interest in data security.

Most data leaks in the Middle East exposed trade and state secrets

The comparison of compromised information by type revealed significant difference between the global and Middle Eastern leakscapes. While almost 67% of all global incidents over the reporting period affected personal data, the majority (over 38%) of Middle Eastern data breaches compromised trade secrets and know how (Figure 1), with a significant share of state secrets being also exposed in the region.

> *Sudanese Mineral Resources Company (SMRC) initiated an investigation into a trade secret leak to social media by its employee. The document compromising may affect the Ministry of Finance, Ministry of Natural Resources, and the Bank of Sudan, which all cooperate with SMRC*
>
> ***SudanNow***

This is due to poor data loss protection of Middle East government agencies and manufacturing enterprises. A relatively small share of personal data leaks in the region (29.6%) is due to the fact that neither criminals, nor media take interest in this data type, with just a few leaks having taken place (particular through external attacks) and a few personal data compromising incidents being reported.

Political and economic conditions in the Middle East, caused by tensions among neighboring countries, influence the big picture of data breaches. Moreover, having energy commodities as their biggest export revenue source, the Middle East countries see public uproar when information of political or technological value is compromised as a result of either external attacks on government agencies and manufacturing enterprises or malicious/negligent actions by their employees.

External attacks are the main cause of data breaches in the Middle East

Two thirds of all leaks from Middle East companies are triggered by external intruders, while

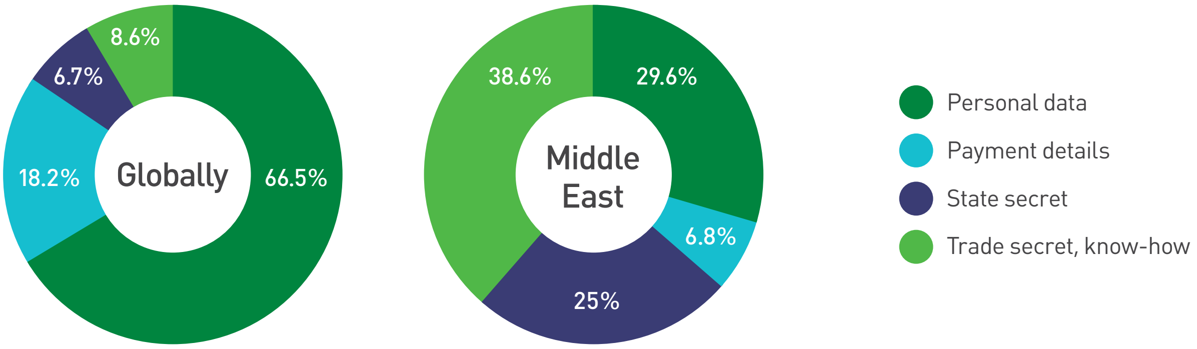

Fig. 1. Types of compromised data

insiders account for almost the same share (62.8%) worldwide (Figure 2).

> *In Lebanon, hackers were arrested for the largest series of attacks in the country's history. The investigation found that cybercriminals stole and sold information of private companies, public institutions, law enforcement agencies, and a major telecom carrier*
>
> ***New Lebanon***

It is important to note that many cybercriminals here are politically rather than economically motivated.

> *Chafer, an Iran-based hacker group, staged anumberofambitiousattacksonorganizations in the Middle East, leveraging new tools such as EternalBlue exploit which was developed by the U.S. National Security Agency and previously used as part of WannaCry and NotPetya cyberattacks. Chafer was focused on gathering information and espionage, hitting organizations in Israel, Jordan, the United Arab Emirates, and Saudi Arabia*
>
> ***Symantec***

A quite small share of internally triggered data leaks in the Middle East should be subject to reasonable doubt. The majority of such incidents compromised extremely sensitive data — state and trade secrets. Insider actions can lead to severe consequences, even death of people and heavy damage to national defense capability.

> *Iran has sentenced to death a person found guilty of providing information to Israel to help it assassinate several senior nuclear scientists, Tehran's prosecutor said. At least four scientists were killed between 2010 and 2012 in what Tehran said was a program of assassinations aimed at sabotaging its nuclear energy program. Iran hanged one man in 2012 over the killings, saying he had links to Israel*
>
> ***Reuters***

In the Middle East, not only government agencies, but also private businesses rarely go public with cybersecurity violations, and even when they do, the usual case is that guilty persons have already been identified and penalized.

> *South Sudanese law enforcement agents arrested deputy accountant of the state-owned oil company (Nilepet) over allegations of leaking confidential documents regarding its operations. In particular, the documents might contain information on corrupt dealings within this national oil company.*
>
> ***Sudan Tribune***

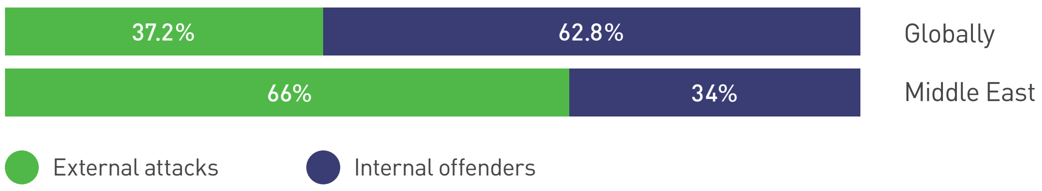

Fig. 2. Attack vectors

A vast majority of internal violations are intentional

The internal leak breakdown by intent shows how poorly Middle Eastern companies are protected against malicious employees. Thus, approximately 85% of all registered incidents are of intentional nature here, compared to almost 69% of accidental leaks globally (Figure 3).

Advanced security tools are, of course, more effective against accidental data breaches. Intentional leaks are mainly recorded when made public. The fact that the majority of Middle Eastern leaks are malicious by their nature allows us to conclude that local companies either fail to identify accidental leaks using their security tools or, as we mentioned above, avoid going public with such incidents.

Rank-and-file employees are behind some 20% of leaks in the region under review, with local top managers (privileged users) accounting for more incidents than their peers worldwide (5.4% vs. 2.2%) (Figure 4).

> *In Algeria, ex member of parliament Ahmed Belkasmi was sentenced to five years in prison for handing over stolen confidential information to a foreign state, including reports on security, economic, and political matters, as well as information on health, movements, and ongoing activities of the President of Algeria.*
>
> ***Alyaoum24.com***

External attackers are responsible for 73% of all recorded data breaches. The analysis of reported data leaks shows that hackers are primarily interested in national strategic plans, know-how, university test papers, etc.

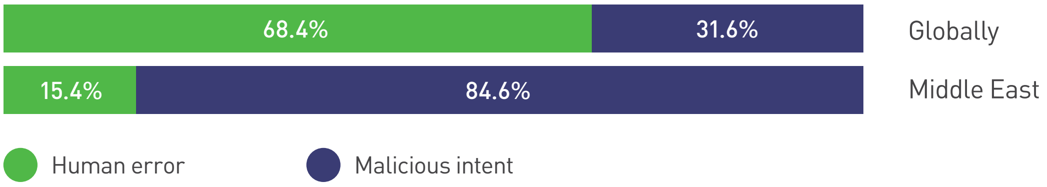

Fig. 3. Causes of data breach

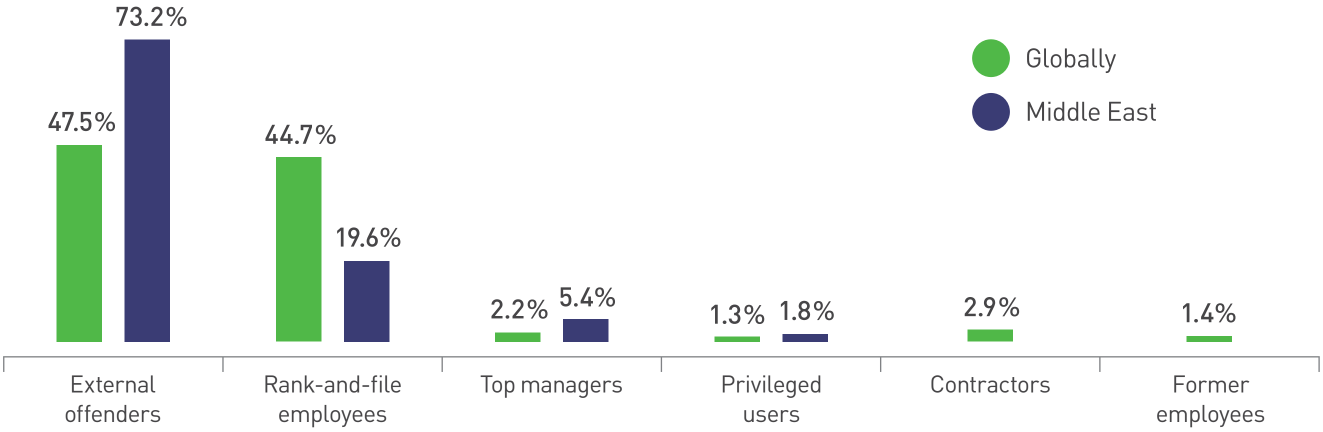

Fig. 4. Types of violators

> *Hackers broke into an email account of a Dubai-based car dealer and altered a delivery address for four Mercedes vehicles, but officers from the Cyber Crimes Department arrested intruders and ruined their plans.*
>
> ***Gulf News***

Although their motives differ, criminals most often seek personal gain.

> *The National Security Service of Iraq arrested an 8-person gang for gaining access to confidential information, such as exam questions issued by the Ministry of Education, and then selling it on social media.*
>
> ***Elaph.com***

Government and banks suffer over 50% of all leaks

There is a huge difference between global and Middle East leak breakdowns by industry. Thus, local government agencies and educational institutions experienced 36% and 20% of leaks, respectively (twice as many as worldwide average). Moreover, compared to global statistics, the region under review also saw more data breaches in banks (15.9%), manufacturing and transport (13.6%) sectors (Figure 5).

> *The UAE Central Bank sent a circular to local and foreign banks and finance companies operating in the UAE, declaring that credit card numbers, email addresses and mobile numbers of around 250 customers based in Dubai had been compromised. As a result, some UAE residents shared their harrowing stories about card frauds they faced after transactions at shopping malls, gas stations, and online stores.*
>
> ***Khaleej Times***

At the same time, the Middle East recorded virtually no leaks from the healthcare, retail, and HoReCa sectors. In our opinion, this is mainly due to the fact that neither hackers nor insiders take a great interest in these data yet. It can also be that companies operating in these sectors simply fail to detect their data leaks, or reported breaches attract no public attention for the reasons mentioned above.

Enterprise leak breakdown by channel differs dramatically in the Middle East and globally. The network channel accounted for over 60% of data

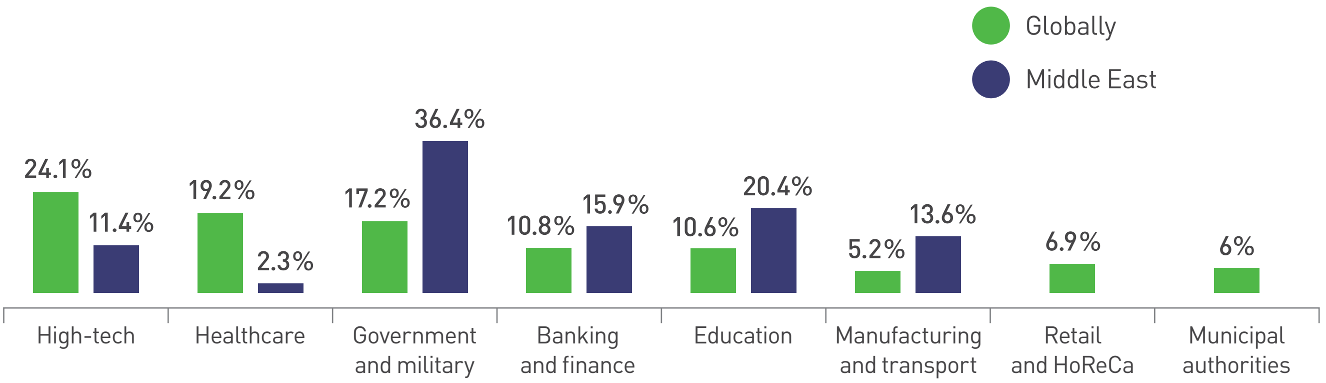

Fig. 5. Insider leaks by sector

leaks worldwide and just 42% in the Middle East. At the same time, the shares of leaks through mobile devices and instant messengers in the Middle East were several times larger than global figures (6.7% vs. 1.9% and 17.8% vs. 4.5%, respectively). Leaks as a result of paper document theft/loss accounted for some 18% of recorded incidents (compared to as little as 11% in the world) (Figure 6).

The share of network channel is half the worldwide size, with almost 25% of leaks going through mobile devices and instant messengers

> *Ahead of the parliamentary elections, two Lebanese embassies abroad have exposed the personal data of Lebanese voters. First, the Lebanese embassy in the UAE sent an email to Lebanese residents with an attached spreadsheet containing the personal details of more than 5,000 Lebanese citizens who have registered to vote in the upcoming elections. Around the same time, the Lebanese embassy in the Hague (The Netherlands) sent a similar email to more than 200 recipients. The email contained an attached spreadsheet with the personal data of the Lebanese voters in the Netherlands. Moreover, the person who sent the email entered all the recipient addresses in the Cc field instead of using the Bcc field to conceal these data.*
>
> ***Smex.org***

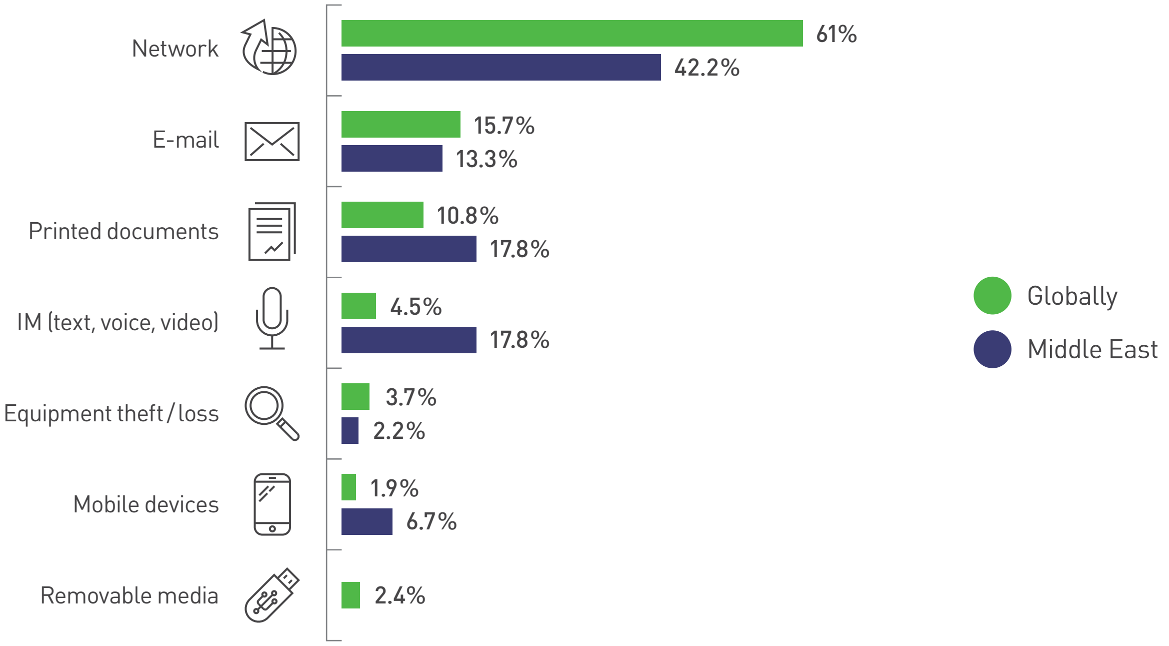

Fig. 6. Data leak sources

CONCLUSION AND FINDINGS

The analysis of confidential information leaks revealed in the Middle East countries shows some key cybersecurity trends. We believe the cyber landscape in this macroregion, like nowhere else, depends on relations among its neighboring states and rather non-public nature of business in most of its countries.

Indeed, as global powers are interested in the region, the Middle East also sees multiple collisions between neighboring governments. National intelligence agencies and hacker groups primarily chase military secrets, information on mission-critical infrastructure facilities, trade secrets of large companies in the Middle East and bordering countries. That is why know-how, state and trade secrets account for the largest share of data leaks here.

Note that external leaks hit the Middle East twice as often as internal ones, which may be attributed to both hyperactivity of cybercriminal groups and political motivation behind many attacks. However, for governments, businesses, and citizens, internal leaks are just as dangerous, despite their relatively small share. Intentional data leaks that most often compromise state secrets and valuable business information account for 85% of all recorded incidents.

The analysis of publicly available cases shows that government agencies and most businesses in the Middle East lack reliable tools to protect themselves against both external and internal leaks. Security services most likely do not notice a great majority of breaches. Moreover, local organizations still have not got used to reporting data breaches. These incidents are usually considered as extraordinary political events here, with businesses and government agencies often failing to see a direct correlation between a confidential information leak and financial and reputational losses.

To prevent data leaks, Middle East companies need to reconsider their security approaches, including both ideology and use of particular external and insider threat protection tools that should combine Data Loss Prevention (DLP) with User and Entity Behavior Analytics (UEBA).

LEAKAGE MONITORING ON THE INFOWATCH WEBSITE

InfoWatch Analytics Center regularly posts data leakage reports on its website, as well as the most notorious incidents commented by InfoWatch experts.

In addition, the website contains data leakage statistics for past years, available in the form of dynamic diagrams.

www.infowatch.com/analytics

Follow the leakage news, new reports, analytical and popular articles via our channels:

https://infowatch.com/subscrybe

https://www.facebook.com/InfoWatchMiddleEast

https://twitter.com/infowatch_me

https://www.instagram.com/infowatch_me

GLOSSARY

Information security incidents *in this research mean cases of compromising confidential information as a result of data leaks and/or destructive actions by employees.*

Data leak *means losing control over information due to external intrusion (attack), access abuse, or unauthorized access.*

Destructive actions by employees *mean personnel actions that resulted in the compromising of confidential information, including the use of confidential information for personal needs associated with fraud; illegal access to information (abuse of access rights).*

Confidential information *in this context means information which can be accessed by a limited number of expressly identified persons subject to its non-disclosure to third parties without the consent of an information owner. In this report, the term "confidential information" also includes personal data.*

Intentional/Accidental Leaks.
<u>Intentional leaks</u> mean an information leakage when a user, who works with information, could foresee negative implications of his or her actions, knew about their illegal nature, was warned about liability, and acted for personal gain or benefit. This results in a risk of losing control over information and/or committing a confidentiality breach. In this case, it does not matter whether such user's actions actually led to negative consequences or corporate losses.
<u>Accidental leaks</u> mean information leakages when a user neither foresees negative implications of his/her actions, nor acts for personal benefit. In this case, it does not matter whether such user's actions actually led to negative consequences or corporate losses. The terms "intentional/malicious" and "unintentional/accidental" are equal and used as synonyms herein.

Attack vector *means a classification criterion of intruder's actions behind data leakage, including intruders who attack company's web assets and IT infrastructure from the outside to compromise data, and insiders who obtain unauthorized access to classified resources and misuse confidential information, etc.*

Data channel *means a scenario which results in the loss of control over information and a breach of its confidentiality. Currently, we identify eight separate leak channels:*

- *Theft/loss of equipment (server, data storage, laptop, desktop), with information being compromised during maintenance or due to the loss of such equipment*
- *Mobile devices where data leakage occurs because of unauthorized use or theft of a mobile device (smartphone, tablet) when used as part of BYOD paradigm*
- *Removable media loss/theft (CDs, flash drives)*
- *A network where data is leaked via a browser (sending data to personal email, filling in browser forms); unauthorized use of intranet resources, FTPs, and cloud services; and unauthorized information posting on a website*
- *Email, with data being leaked via corporate email*
- *Paper documents which can cause a data leakage if stored or utilized improperly (with confidential information printed, stolen, or taken out)*
- *Instant messengers (data leakage via voice, chat, and video communications)*
- *'Non-defined' is a category used when incident details appearing in mass media do not allow for the leak channel identification.*

INFOWATCH®

15 YEARS
OF PROTECTING
YOUR DATA

Headquarters
Vereyskaya street 29, building 33,
121357, Moscow, Russia
+7 495 22 900 22, +7 499 37 251 74

InfoWatch Labs
Level 33, Ilham Tower, No. 8, Jalan Binjai,
50450, Kuala Lumpur, Malaysia
+603 2117 5177, +603 2117 5178

InfoWatch Gulf
Suite 3203, 1 Lake Plaza Building, Cluster T,
Jumeirah Lake Towers, Dubai, UAE
+971 4 558 65 65

iw-global@infowatch.com
www.infowatch.com