SECURITY REVIEW REPORT

July '18

Content

1

Developments within the Period

a. In Turkey:

(1) Cyber attack to the company's account

An international trade company reported to the İstanbul Police Department Cybercrime Branch teams that 11 million 231 thousand euros from the company's account has been transferred and that the company officials had no information about this transfer.

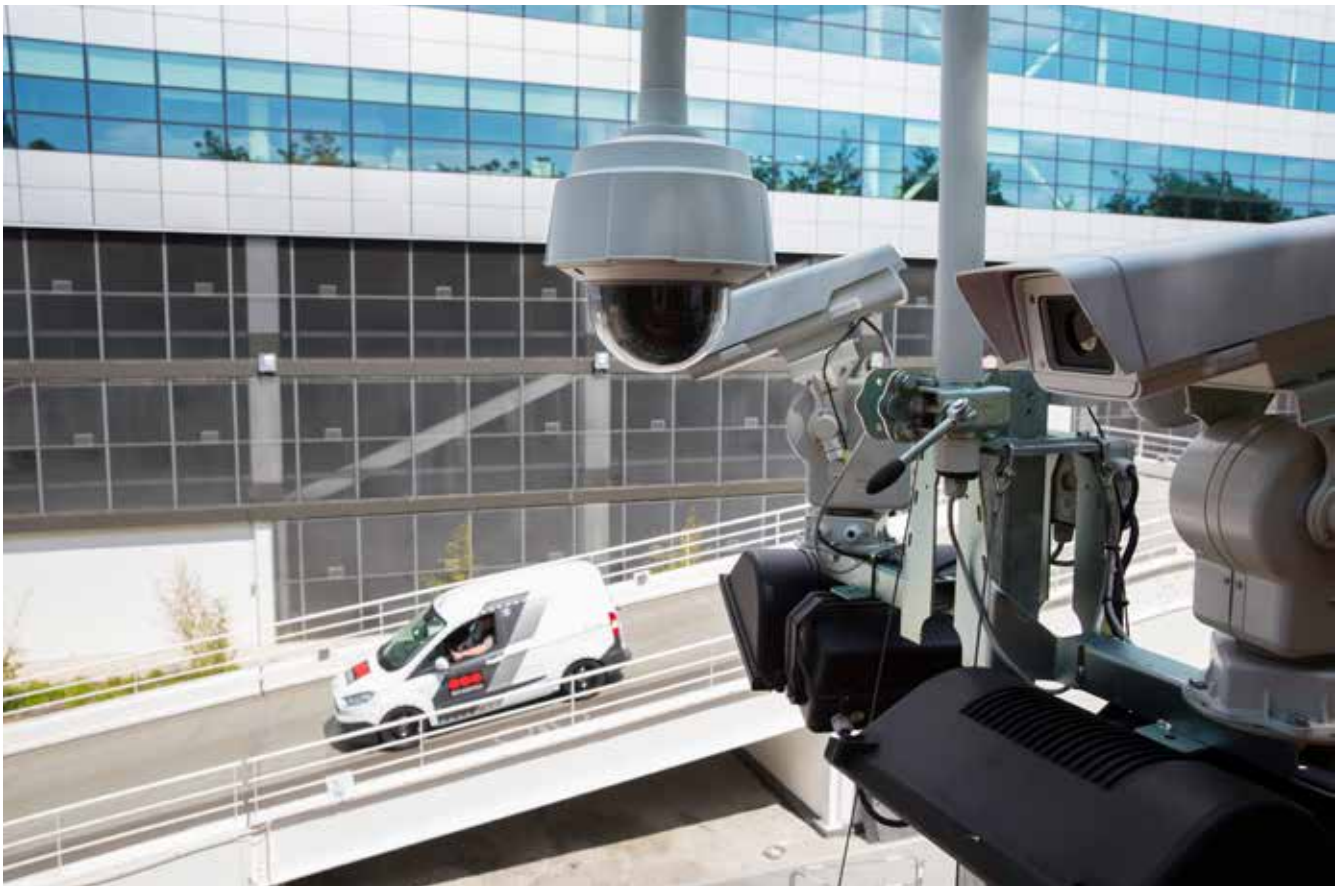
The police detected that the mail accounts of company was hacked using "Man in the middle" (monitoring the connection between two ports) attack method. Three people, including foreign nationals, were arrested while eight suspects were released on conditional judicial control.

(2) Drug operation in Kayseri

On June 22, 2018, 233 kilogram heroin, which is concealed inside the chestsand planned to be exported abroad in furniture, were seized by the teams of the Narcotic Crimes Branch Office in Kayseri.

(3) New period in shopping malls in Ankara

Ankara Police Department has opened police liaison offices in 25 shopping malls in Ankara in order to ensure that the security services such as body search at entrances, vehicle check, bag and package control and perimeter security are carried out more controlled and properly. Within the scope of the application which is



coordinated with the administrations of the shopping malls, the security inspections will be carried out permanently in shopping malls by civil teams in the liaison offices consisting of two or more personnel connected to the Directorate of Private Security Branch.

(4) Accident report during the Eid al-fitr

Between June 15 and 17, 2018, 58 people lost their lives and 392 other were injured in traffic accidents during the Eid al-fitr in Turkey.

(5) Operations against ISIS terorist organization

- On May 30, 2018, 1 Syrian national suspect was taken into custody in the operation against ISIS terrorist organization in **Elazığ**.
- On May 30, 2018, 6 Iraqi national suspect were taken into custody in the operation against ISIS terrorist organization in **Samsun**.
- On May 31, 2018, 20 ISIS suspects, including 6 foreign nationals, have been caught in **Sakarya**.
- On May 31, 2018, 28 hand granades, 5 automatic weapons and magazines, and a large number of bomb pieces belonging to the ISIS terrorist organization were found in the searches made jointly by police and gendarmerie teams in the region close to the Syrian border in **Hatay**.

1

Developments within the Period

- On June 2, 2018, 51 suspects have been detained in the operations against ISIS terrorist organization in **Istanbul**.
- On June 8, 2018, 5 suspects have been detained in the operations against ISIS terrorist organization in **Kocaeli**.
- On June 11, 2018, 13 suspects have been detained in the operations against ISIS terrorist organization in Adana.
- On 13 June, 2018, 1 ISIS member have been arrested by the court in **Manisa**.
- On June 14, 2018, 8 suspects have been detained in the operations against ISIS terrorist organization in **Istanbul**.
- On June 14, 2018, 4 suspects have been detained in the operations against ISIS' Tevhid magazine in **Istanbul**.
- On June 16, 2018, 30 people, the majority of whom were foreign nationals, were detained in **Istanbul**, in the operation against the terrorist organization ISIS.
- On June 18, 2018, 1 suspect has been detained in the operations against ISIS terrorist organization in **Ankara**.
- On June 22, 2018, 14 people have been detained in the simultaneous operations against ISIS in **Ankara** for allegedly being in search of action before elections.

b. In the World:

(1) Bombed vehicle attack in Afghanistan

On June 16, 2018, Interior Minister of Afghanistan Veys Ahmed Barmak met with unarmed Taliban militants in Kabul, Afghanistan's capital city. After hours, the Kabul administration announced that the ceasefire during the Eid al-fitr was extended. 46 Taliban militants in prison were released.

The Taliban declared a ceasefire for the first time during the Eid al-fitr, and the Afghan government took a step for a specicific period.

On the other hand, at least 26 people were killed after the explosion of a bomb-laden vehicle whereTaliban militants and soldiers gathered in the city of Nangarhar. ISIS claimed the responsibility for the attack.

(2) Hand Granade Attack on the Ethiopian Prime Minister

On June 23, 2018, during the speech of new Prime Minister of Ethiopia, Abiy Ahmed, at Meskel Square, where tens of thousands of people gathered, a hand granade attack was carried out by a man whose identity could not be determined yet.

100 people were injured in the attack while Prime Minister Abiy Ahmed saved without getting wounded.

2 Cross-border Operations

Within the scope of information provided by the Turkish Armed Forces;

a. Medium-scale operations continue in Şırnak and the northern part of Iraq, where the PKK/KCK terrorist organization has used as a transit route.

b. Operation Olive Branch: Mine and handmade explosives cleaning activities continue in Afrin, which is under control as of 18 March 2018. As of today, 240 mines and 1276 handmade explosives have been identified and destroyed.

4.509 terrorists have been rendered ineffective since the beginning of operation.

c. Operation Euphrates Shield: In additon to the bomb and mine sweeping activities in the Bab region, contribution to normalization process (infrastructure, superstructure, support of local governments, etc.) continue in the region.

d. İdlib Region 12 observation points were established by the Turkish Armed Forces since October 13, 2017. Turkish Armed Forces units continue to carry out their duties in the region in accordance with the agreed rules of engagement in the Astana negotiations.

e. Manbij Region: Independent patrol activities have started on June 18, 2018 by the Turkish Armed Forces and the US Armed Forces on the line between the Operation Euphrates Shield Area and the Münbic region.

**Compiled within the framework of information obtained from open sources. It is informative only.*

3 Security Assessment

The operations of the Turkish Armed Forces in the northern part of Iraq and in Syria, especially against the PKK and ISIS terrorist organizations, continue. Besides, activities of mine and handmade explosive sweeping, humanitarian aid and providing suitable living conditions for the people of region go on within the scope of operations in Syria.

On the other hand, the operations of the security forces in the Eastern and Southeastern Anatolia regions and northern part of Iraq towards the PKK terrorist organization continue. The PKK terrorist organization has recently increased attacks to various military bases, police stations in Turkey, and especially in northern Iraq.

It has been assessed that, the PKK terrorrist organization may continue its attacks primarily towards the police and military units in order to interrupt the ongoing operations.

Within the scope of operations carried out against terrorist organizations in Turkey, it is observed that the detentions of the members of PKK, ISIS, El-Nusra, Al-Qaida and far left organizations continue intensively. In particular, recent arrests took place mostly in big cities. It has also been been observed that the so called senior officials, who are in the Ministry of Interior's Terrorist Wanted List, are among the detained members of the organization. It is assessed that the members of these organizations may take actions when they find the opportunities to carry out.

In this context, it has been assessed that, as the terrorist organizations lose power due to the operations being carried out, they may be in search of directing their organizational activities to city centers and seeking to carry out actions directed towards the places like shopping malls or public transportation systems (port, station, subway, airport, bus station etc.) where people use intensely.

On the other hand, the June 24th elections completed and there was no significant incident before the election and the ongoing period following the results of the election. No major developments are expected within the scope of election sensitivities in the coming days.

The developments related to these sensitivities will be followed by us and the necessary information will be shared via SMS and e-mail when needed.

4 Statistical Information Concerning the June 2018 Period:

Terror Operations;

According to the weekly reports published by Ministry of Interior about the operations within the country;

- Between May 21-28; 41 PKK/KCK members, 1 DHKP/C member,
- Between May 28-June 04; 29 PKK/KCK members, 1 ISIS member,
- Between June 04-11; 69 PKK/KCK members,
- Between June 11-18; 20 PKK/KCK members, 2 ISIS members,
- Between June 18-25; 22 PKK/KCK members, 2 ISIS members,

Totally **187 terrorists** have been rendered ineffective.

In addition;

- Between May 21-28; 145 PKK/KCK members, 33 ISIS members, 7 FAR LEFT members,
- Between May 28-June 04; 232 PKK/KCK members, 43 ISIS members, 9 FAR LEFT members,
- Between June 04-11; 234 PKK/KCK members, 37 ISIS members, 8 FAR LEFT members,
- Between June 11-18, 134 PKK/KCK members, 61 ISIS members, 12 FAR LEFT members,
- Between June 18-25; 395 PKK/KCK members, 68 ISIS members, 3 FAR LEFT members,

Totally **1.421 suspects** have been arrested.

b. Public Order Operations;

Between May 21-June 25, 2018, in the **13.067** operations conducted to fight against "Drug and Smuggling";

5.015 kg Marijuana

1.613 kg Heroin,

3 kg Cocaine,

17 kg Synthetic cannabinoid substance,

2.308.292 packs smuggled tobacco,

315.052 liter fuel oil.

19 kg Methamphetamine,

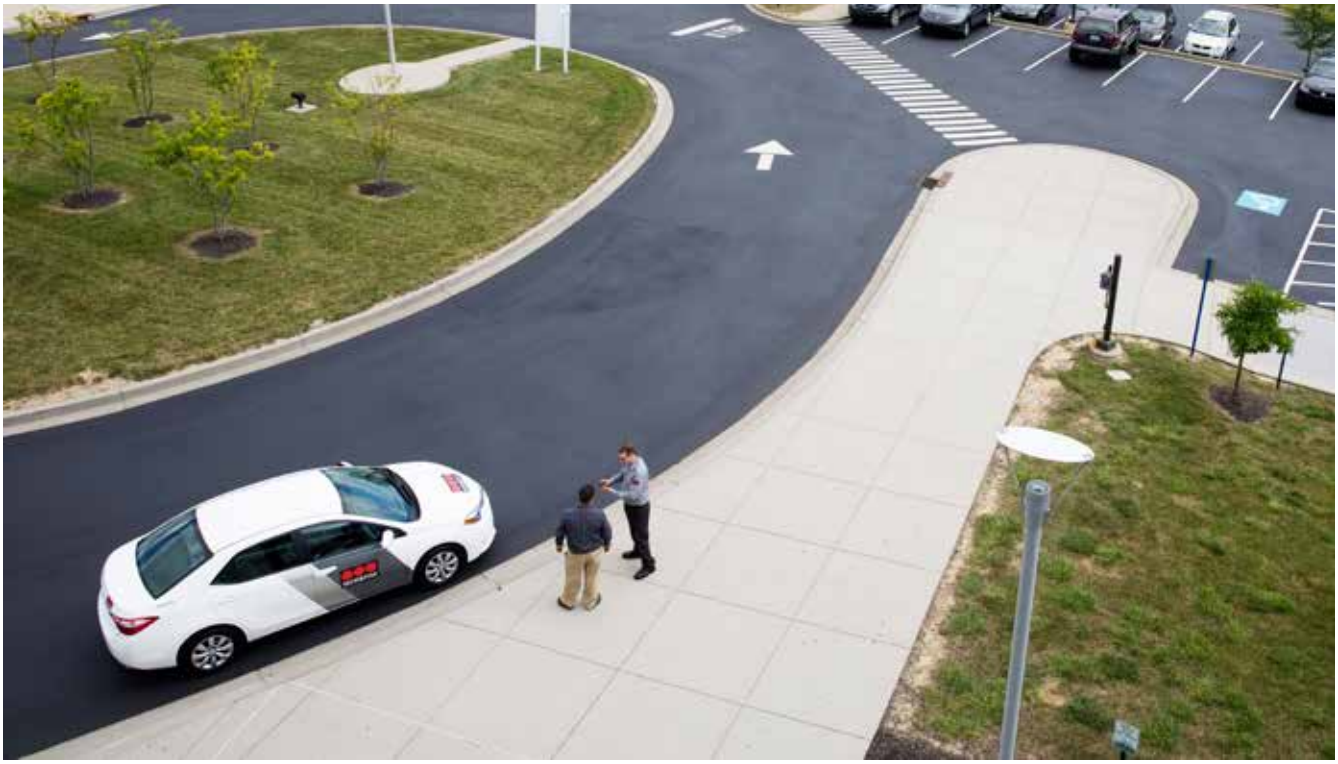
3.614.410 pieces Tabloid drugs

440.864 Cannabis plant

were seized.

Within the scope of the operations, **16.951** people were taken into custody.

* www.icisleri.gov.tr



5 Important Days and Weeks in July 2018:

DATE	INCIDENT
July 02, 1993	Sivas Incidents
July 07, 2005	Londra Subway Attacks (ISIS / 52 deaths, 770 casualties)
July 04, 2016	Medine Mescid-i Nebevi Attack (ISIS / 6 deaths, 10 casualties)
July 14, 2016	France Nice Attack (ISIS / 84 deaths, 202 casualties)
July 15, 2016	Coup Attempt (FETÖ)

There is no day with high security sensivity in July, however, It has been assesed that the sensivity will keep its importance across the Turkey due to the operations carried out against terrorist organisations, particularly PKK and ISIS, within the country and out of borders and the security measures taken in this period should be reviewed.

Additional Measures:

The measures to be taken in addition to the existing measures will be announced to you in addition to the "Securitas Security Assessment" by our relevant Branch Manager taking into account the sensitivity of the period.

6

Highlight of the Month

Dear Business Partner,

Securitas Security Services and Pronet Security and Consultancy have agreed to join forces under the brand of Securitas and both parties reached an agreement on May 31, 2018.

The purpose of this acquisition is to build the top security service provider in Turkey.

We believe that the value added resulting from the acquisition, based on the strongest aspects of both companies, will benefit both the security services sector in Turkey, and your company as well.

During the process Securitas will continue to provide its services with the same understanding of quality and standarts.

We hope this acquisition will benefit you and the sector as a whole as well.

By the Numbers

The increase of the **Cryptojacking Attacks in 2017 is 8,500%**

%8,5K

%92

92% of malware is delivered via email.

69% of organizations don't believe their antivirus can stop the threats they're seeing.

%69

* www.symantec.com
* www. barkly.com
* www. barkly.com

7

Security First

The Relationship Between Physical Security And Information Security

In some risk management situations, the link between physical security and information security is often overlooked and not appreciated. This disconnect is often a two-way street where information security managers neglect the dangers and vulnerabilities posed by physical security lapses; while physical security managers avoid the seemingly complex and intimidating practice of securing information. This article looks to bridge the link between the two by exploring the role of physical security in an information security management system.

Information security management systems are business management systems that aim to protect information from unauthorised access, use, disclosure, disruption, modification, recording or destruction. It is a common misconception that information security management systems are built only to prevent hackers from gaining access to a computer or network. On the contrary, an information security management system is meant to protect the integrity, confidentiality, and availability of information. A successful information management security system will protect and secure information of all types, whether it be printed, written, stored electronically, spoken, presented in video or audio format, or sent via post or email. An information management security system ensures information, no matter how it is transmitted, shared or stored, is always protected in an appropriate manner.

7 Security First

The protection of information does not stop by simply ensuring that ample, virus-protection software and strong firewalls are established. Information security also includes establishing a thorough physical security system as well. The goal of a physical security management system, in terms of information management security, is to prevent unauthorised physical access, damage and interference to an organisation's premises and information.

In establishing a physical security system for ample protection of an organisation's information, the following questions should be addressed:

- Does your organisation have a physical security policy?
- Does this policy address the following?
  - Campus security?
  - Building security?
  - Floor security?
  - Room security (including data and wiring closets)?
  - Asset security?
- Are controls in place to physically protect the classification of information and information technology?
- Are controls in place to ensure the use of appropriate identity and privilege credentials?
- Are physical barriers present (fences, gates, walls, exterior doors, windows, interior doors)?
- Are the physical premises monitored for fire, flood, intruders and temperature fluctuations?
- Are appropriate controls in place to serve as physical barriers, such as vehicle barriers, card readers and combination locks?
- Is a log entry and exit system in place?
- Are video monitoring systems, motion detectors, proper lighting and guards (when appropriate) in place, as needed?

Most of these questions are rather intuitive, such as ensuring there are exterior doors and windows on an office building. However, physical security requires further measures to ensure that information is not

7
Security First

accessed by unauthorised parties. For example, when labelling interior doors, it is more prudent to label the room as Room 3A as opposed to Data Centre.

Once these questions have been addressed and controls have been put in place, it is necessary to test these mitigating controls through penetration testing. Penetration tests aim at assessing the vulnerabilities of information, assets, and the physical security system as a whole. Simply creating controls does not ensure the controls will prevent unauthorized access and security breaches. Penetration testing exposes errors in the physical security system, especially the most common issues of risk associated with human error.

In order for a control to be successful, employees must understand the ins and outs of the mitigating controls and why they have been put in place. Education, information and awareness training of employees are elements vital to ensuring the success of any security management system. In order to understand the comprehension and level of awareness of employees regarding controls, penetration tests should be carried out continuously.

An example of a penetration test would be to have an individual from outside of the organisation attempt to gain access to the organisation's secured information. This individual, dressed as a technician visiting the organisation to do something as simple as read electricity-use meters or test the voltage of certain power outlets, then attempts to access secure information held by the organisation.

7

Security First

A successful physical security system would be able to stop this individual at the early stages of entry. For example, a secure, entry and exit card reader would prevent the individual from entering the premises without the necessary approval. However, this is not always the case and the individual, dressed in his or her technician's outfit, often establishes credibility. Next, the pretence used often fools employees into being more than willing to assist the technician to complete his stated task, giving him free rein to otherwise-secure areas of the organisation's premises.

During such penetration tests, employees have allowed the technician to place hacking devices and collect data. They have often left their desks unattended, allowing the technician access to their computer and the physical information on their desk. In some cases, the bogus technicians have even been given access to data centres containing all of the organisation's confidential information.

When penetration test are carried out, weaknesses and vulnerabilities are exposed. As stated, these weaknesses and vulnerabilities often exist as a result of human error. In all forms of risk management, whether it be information or physical security risk management, employees or human factors are the ultimate source of risk. In order to merge the physical and information security elements into a successful system, measures must be taken to reduce human error and its associated risk. This can be possible if sufficient effort is put into raising the level of awareness of the organisation's security policies and procedures and staff training to minimise human-factor risks.

Both information and physical security managers should develop training sessions tailored to the responsibilities of employees and which highlight vulnerabilities such as those revealed by penetration testing results. Successful training will embed a culture of risk management regarding both physical and information security, and ensure that employees consciously consider the risks their actions often pose to the organisation.

Beyond training sessions, additional policies that include a disciplinary process should be put in place. A disciplinary process for breaches of an organisation's security is necessary to establish the importance of security to the organisation. The objective of the disciplinary process is to bring attention to, and have consequences for security breaches.

This article has focused primarily on the role of physical security in the protection of information. Often, the notion of information security is viewed as complex and consequently left to the IT guys.

7

Security First

However, although some aspects of information security requires a deep understanding of technology (both hardware and software), the general idea of protection is similar to that of physical security. For example, requiring employees to have a unique, user login and password to access a company computer and the local network is no different from requiring an employee to enter the office using an ID card with a photograph. In order to ensure a proper bond between information security and physical security, the physical security managers should familiarise themselves with the controls put in place to protect information outside the realm of physical access.

The purpose of this article is to stress the importance of the unification of information security policies and physical security policies. In order for an organisation to protect one of its most important assets, information, that unity between the two disciplines is necessary. Through penetration testing, education, awareness and disciplinary action, when necessary, security managers can ensure the well-being of the information, staff, and assets held by the organisation.

www.securitysolutionsmedia.com

8

Securitas Guidelines for Secure Life

In this section, we would like to inform you about practical security measures to be taken at home when you go on vacation or business trip.

Taking into account the following points will help to ensure your safety.

Practical Security Measures to Take at Home During Holidays or Business Trips

- Have 24-hour online Electronic Security Systems installed at home by certain centres.
- If you will be away from the house for extended periods of time on business or for pleasure, ask your neighbours to help you with the collection of newspapers, letters, invoices or similar documents piling up in front of your door or in you letter box.
- Use a "TIMER" to turn on the lights around the house and your radio or television automatically at certain intervals.
- Remove any names on the door or on the letter box.
- Never leave your spare key under the door mat, in letter boxes or in pots outside the house, etc.
- Do not let many people other than your close neighbours know that you will be out of the house for some time. Provide a telephone number and address for your destination only to people you sincerely trust.
- Before leaving your house, turn of all taps and valves including water and gas lines or LPG tank, etc.
- If your house has been subject to a robbing despite the measures you have put in place, call 155 Police Hotline or 156 Gendarmerie Hotline from the closest telephone without panicking or touching any furniture or door. Try to provide officials with as much information as you can.

We wish you safe and healhy days.

Best Regards.


SECURITAS


SECURITAS