

# ME cybersecurity prominence - 2021



---

Amin Hasbini



## Amin Hasbini

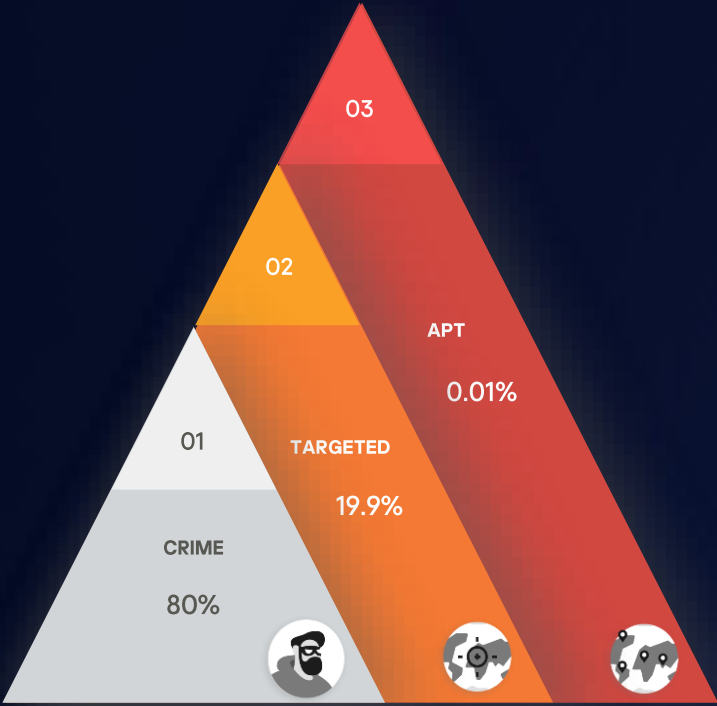
- Director of research center META, Kaspersky
- PHD smart cities security, Brunel University London
- Threat Hunter

# Agenda

1. Cybersecurity governance
2. Regional statistics
3. Future predictions

# Cybersecurity governance

# Kinds of threats targeting users and organizations



# Understanding cybersecurity governance

\_\_\_\_\_ ISO and IEC definition

\_\_\_\_\_ Cybersecurity governance Vs Cybersecurity management

*"The system by which an organization directs and controls security governance, specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks."*

# Cybersecurity governance essentials

- \_\_\_\_\_ Aligning cybersecurity with business objectives
- \_\_\_\_\_ Defining policies, procedures and frameworks
- \_\_\_\_\_ Defining cybersecurity decision making hierarchy
- \_\_\_\_\_ Defining accountability for decisions
- \_\_\_\_\_ Ensuring feedback is collected for decisions
- \_\_\_\_\_ Ensuring compliance with regulatory requirements
- \_\_\_\_\_ Monitor, measure, analyze, report and improve

# Cybersecurity governance main challenges

- \_\_\_\_\_ Industry requirements (contractual, legal, regulatory)
- \_\_\_\_\_ Environment requirements
- \_\_\_\_\_ Pervasive agility



# ME threat statistics



## Web attacks blocked in H1 2021 (Jan->Jun)

Country	Total
Saudi Arabia	46.6M
United Arab Emirates	19.9M
Oman	12M
Turkey	30M
Egypt	28.9M
Jordan	6M
Lebanon	5M
Pakistan	6M
Algeria	79.4M
Morocco	29.1M

GREAT

Source: Kaspersky Security Network (KSN)

kaspersky

# Malware attacks blocked in H1 2021 (Jan->Jun)

Country	Total
Saudi Arabia	780k
United Arab Emirates	3.8M
Oman	270k
Turkey	24M
Egypt	700k
Jordan	260k
Lebanon	260k
Pakistan	440k
Algeria	400k
Morocco	740k

# Banking trojans blocked attacks in H1 2021 (Jan->Jun)

Country	Total
Saudi Arabia	23k
United Arab Emirates	36k
Oman	3k
Turkey	83k
Egypt	39k
Jordan	4k
Lebanon	3k
Pakistan	65k
Algeria	79k
Morocco	17k

GREAT

Source: Kaspersky Security Network (KSN)

kaspersky

# Ransomware trojans blocked attacks in H1 2021 (Jan->Jun)

Country	Total
Saudi Arabia	43k
United Arab Emirates	24k
Oman	5k
Turkey	128k
Egypt	107k
Jordan	44k
Lebanon	3k
Pakistan	110k
Algeria	48k
Morocco	20k

GREAT

Source: Kaspersky Security Network (KSN)

kaspersky

## Top impacted cities

Country	Total
Saudi Arabia	Riyadh, Mekka, Eastern province
United Arab Emirates	Dubai, Abu Dhabi, Sharjah
Oman	Muscat, alBatina, Dhofar
Turkey	Istanbul, Ankara, Izmir
Egypt	Cairo, Alexandria, Qalyubia
Jordan	Amman, Alzarqa, Irbid
Lebanon	Beirut, Mount-Lebanon, North-Lebanon
Pakistan	Punjab, Sindh, Islamabad
Algeria	Alger, Tipaza, Setif
Morocco	Casablanca, Rabat, Marrakech











GREAT

kaspersky

Source: Kaspersky Security Network (KSN)

---

# Top 10 targets

-  Government
-  Banks
-  Financial Institutions
-  Diplomatic
-  Telecommunications
-  Educational
-  Defense
-  Energy
-  Military
-  IT companies

---

# Top 10 active threat actors

- |  |  |
|--|--|
|  Lazarus          |  StrongPity       |
|  DeathStalker     |  Sofacy           |
|  CactusPete       |  CoughingDown     |
|  IAmTheKing       |  MuddyWater       |
|  TransparentTribe |  SixLittleMonkeys |



# Projected threat evolution

An aerial, long-exposure photograph of a city intersection at night. The image shows multiple roads converging, with light trails from cars creating a sense of motion. Buildings and streetlights are visible, and the overall scene is illuminated by the warm glow of city lights.

GREAT

kaspersky



# APT threat actors will buy initial network access from cybercriminals



Targeted ransomware gangs using generic malware, e.g. Trickbot



Links between targeted ransomware groups and underground markets



APT threat actors to follow suit

# Demanding money, threatening and blackmailing

- Ransomware developments
- Including the switch to highly-targeted attacks
- Careful selection of targets, big pay-outs
- No sector off-limits
- Ransomware plus doxing to maximize ROI
- Collaboration of ransomware gangs
- The future will be a blend of established practices and a small number of APT-like gangs

# Increased targeting of network appliances



Improvements in operational security will drive threat actors to look for other vulnerabilities



Including network appliances, e.g. VPNs



Focus on social engineering, including reconnaissance through phishing and other real-world approaches

# More disruptive attacks



Bigger attack surface  
than ever before



More disruptive attacks  
in the future



Either through deliberate  
attack or collateral damage

# The emergence of 5G vulnerabilities

A person is shown in profile, looking down at a smartphone held in their hand. The scene is set at night, with a dark blue sky and silhouettes of trees in the background. The person's face is partially illuminated by the light from the phone's screen.

- 5G has attracted a lot of attention this year
- Concerns about Huawei and fake news about health risks
- Public and private researchers looking at the products of Huawei and others for implementation problems, crypto flaws and even backdoors
- Any flaws found will have massive impact
- Take-up of 5G will give hackers more incentive to look for vulnerabilities to exploit

# Conclusion

**Thank you!**  
**شكراً جزيلاً**

More info:  
[Amin.Hasbini@kaspersky.com](mailto:Amin.Hasbini@kaspersky.com)

**GREAT**

kaspersky