The Arab Cybersecurity Landscape: Challenges and Opportunities

Amro Moussa

The Arab Cybersecurity Landscape: Challenges and Opportunities

The issue of cybersecurity is as vital to our way of life as technology itself. The two are intimately intertwined.

In fact, they can't be separated: our economic health, our national security, and indeed the fabric of our society is now defined by the technology we depend on every day.

The Arab Cybersecurity Landscape: Challenges and Opportunities

It is vital to understand how cybersecurity relates to our national security, our national interest, and our economic prosperity.

Also, how cybersecurity is a driver of productivity, innovation and business

The Arab Cybersecurity Landscape: Challenges and Opportunities

As technology continues to evolve so also do the opportunities and challenges it provides. We are at a crossroads as we move from a society already entwined with the internet to the coming age of eCommerce, digital economy, automation, Big Data, blockchain and the Internet of Things (IoT).

The Arab Cybersecurity Landscape: Challenges and Opportunities

And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyberattacks.

The Arab Cybersecurity Landscape: Challenges and Opportunities

Concerns facing us in the near future will include:

- New attack vectors such as botnets, wearables (smart watches), autonomous cars and ransomware.

- Threats such as data manipulation, identify theft, bringing down websites, stealing data, committing fraud and .. **CYBERWARFARE**.

- Tangential issues such as data sovereignty, digital trails, and leveraging technology talent.

The Arab Cybersecurity Landscape: Challenges and Opportunities

Cybersecurity is not luxury or optional

NOT ANYMORE

The Arab Cybersecurity Landscape: Challenges and Opportunities

Cyber threats combating is a multi-disciplinary affair that spans hardware and software through to national strategies, regulators, law-makers, policies and people – all of it is aimed at both:

- preventing cybercrime occurring in the first place,
- or minimizing its impact when it does.

This is the practice of cybersecurity.

The Arab Cybersecurity Landscape: Challenges and Opportunities

Cybersecurity is a constantly evolving, a constantly active process just like the threats it aims to prevent. Here is where an ongoing operational risk management framework is a vital topic.

The Arab Cybersecurity Landscape: Challenges and Opportunities

Cybersecurity is not luxury or optional

NOT ANYMORE

Cybersecurity is a "national Threat to each nation"

The Arab Cybersecurity Landscape: Challenges and Opportunities

Challenges

Challenges

- National Information Security &
Cyber Security Strategy

(Enforcement and national critical infrastructure as a main challenge – Financial infrastructure & Power infrastructure as an example)

Challenges

- Awareness

Even the most hardened system can be breached through social engineering – the 'hacking' of people. No amount of secure network topologies and firewalls or security software can withstand a user innocently clicking on an email link, or being convinced to give up login details over the phone by someone pretending to be someone else or a source of benefit to the victim - digital literacy.

Challenges

- Education

Information Security & Cyber Security students and professionals are no more just "technicians". They became "business enablers" (business orientation) and strategic stakeholders (operational risk oriented and national welfare oriented)

Challenges

- Collaboration & false sense of security

If there is one lesson we learn from cybercriminals it is this : Collaboration is king. Analysis of attacks over the years has revealed that cybercriminals work together exceptionally well: sharing knowledge of exploits, selling stolen data in an open market, and working together to develop new hacking techniques for infiltration.

(Detection mechanisms, announce and share)

Challenges

- Corruption

(Main enemy to: digital economy (shadow economy), operational risk management as a foundation to any security ecosystem and digital payment systems (logs of payments and digital currency))

Challenges

- Technology-aware law-making and regulation ecosystem

(Parliaments – proper and usefull cyber crime laws and digital fintech services as an example – digital identity, tamperproof trusted digital evidence, digital cash)

Challenges

- Lack of leadership

Lack of leadership is a key challenge, if only because it takes a concerted effort to both recognize and take action on what is clearly a vital function in today's technologically savvy world.

The foundation of any society is trust, as well as the foundation for security itself. Security helps build trust between people and technology. (Actionline C5 – WSIS)

As a result, leadership is required to tackle issues around cybersecurity, governance, private-sector support and education to ensure we can adequately protect the foundation of trust upon which we all depend.

The Arab Cybersecurity Landscape: Challenges and Opportunities

Opportunities

<u>Opportunities</u>

- Job creation
- Trusted platform for a prosperous digital economy

(data-driven economy & economic growth)

Opportunities

- National security protection
- Trusted service delivery platform to achieve SDGs
- Building the secure digital society

The Arab Cybersecurity Landscape: Challenges and Opportunities

Thank you