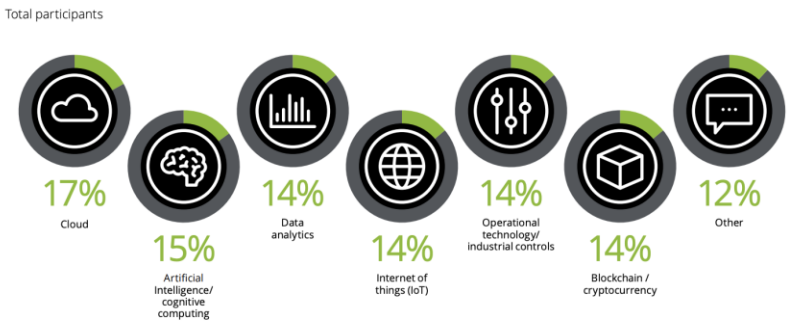
Cyber Security challenges & opportunities in MEA

Reslan Hashim Alabaji
Head of CX SP Customer Delivery, KSA
25 Nov 2020

Cybersecurity digital transformation need

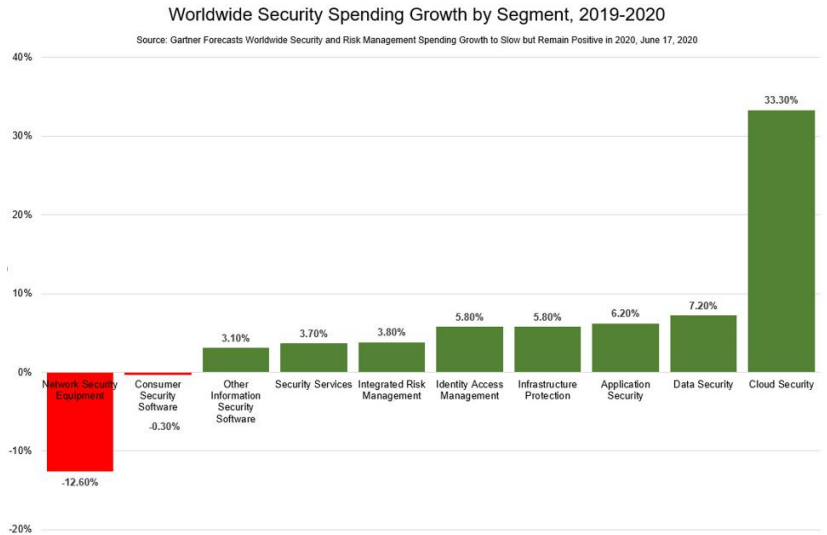
- Top ranked digital transformation initiatives 2019 (Pre-Covid19)



Cyber transformation is the most challenging aspect of cyber risk management for CSOs and CIOs

Ref **Study by Deloitte (2019)

- Forbes Predicts Cybersecurity Spending To Reach $123B of annual revenue worldwide In 2020 where only spending's o cloud security increase by 33%.



**GARTNER FORECASTS WORLDWIDE SECURITY AND RISK MANAGEMENT SPENDING GROWTH TO SLOW BUT REMAIN POSITIVE IN 2020, JUNE 17, 2020

Cloud Security is the smallest, fastest-growing cybersecurity market segment with market size of $439M last year. Its projected 33% growth this year is a function of its small initial market size and organizations' preference for cloud-based cybersecurity solutions. Gartner predicts networking security equipment, including firewall equipment and intrusion detection and prevention systems (IDPS) will be most impacted by the pandemics' hard reset on enterprise IT spending.

Cybersecurity in Middle East

Pre COVID-19 Forecast: The Middle East cybersecurity market market is projected to grow from USD 16.1 billion in 2020 to USD 28.7 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 12.2% during the forecast period in the pre-COVID scenario.

Post COVID-19 Forecast: The Middle East cybersecurity market is projected to grow from USD 15.6 billion in 2020 to **USD 29.9 billion by 2025**, at a Compound Annual Growth Rate (CAGR) of 13.8% during the forecast period in the post-COVID scenario.

From our own experience, there is a huge market requirement, and shortage of qualified resources at the moment in this area. The gap expected to grow in 2021 worldwide.

Kingdom of Saudi Arabia (KSA) held the highest market share during the forecast period

Technological advancements in areas such as cloud, 5G, and IoT and digital transformation are the main drivers to the growth of the market. Also, government regulations, soaring cybersecurity incidents, and cloud technology adoption in the country have contributed to market growth.

*Ref **globenewswire*

The size of Saudi Arabia's cybersecurity market in 2019 was SAR10.9 billion ($2.9 billion) and that market is expected to grow at a CAGR of 16.59 percent through 2023 to an estimated SAR21 billion ($5.6 billion).

*Ref **USSABC*

COVID19 Accelerating effect

- **A rise in COVID 19 related phishing and ransomware attacks**
- **Service Assurance & Business Continuity Plans (BCP) to feature global pandemics**
- **Increased security risk from remote working/learning**
- **Potential delays in cyber-attack detection and response**
- **Exposed physical security**
- **Influx of cyber criminals**
- **Post COVID-19 Cyber Security becoming integral part of business operations.**

In conclusion, COVID-19 will change our lives forever with new work styles, new cybersecurity issues, new proposed policies, personal hygiene and so on. The fight against COVID-19 is not just for the organization, employee or customer but a joint effort from everyone. It is also apparent that Post COVID-19, organizations will need to rethink their cyber risk management measures.

Ref **Deloite March 2020

Cisco's CEO Chuck Robbins talking about fY2021: 'Great Opportunities' Ahead As Businesses Race Toward Digital Transformation

Microsoft CEO Satya Nadella "2 years of digital transformation in 2 months" April 2020

Cisco Security Portfolio

Cisco SecureX Platform

Zero Trust

Security Operations
Breach Defense

Capture the Cloud Transition

Programs, Tools & Solutions

- NetSec Technical Programs
- Cisco Managed Security Offerings
- Secure Access Service Edge (SASE)
- Application First
- Secure Remote Worker
- SAFE
- Security Blueprint
- Industrial / IoT Security
- Modernize the Firewall

CyberSecurity Domains

Cyber Security Domains

Doers (Starting point)

Description

Primarily operations people! These are the guys that keep the lights running in cyber security operations. Think of Firewall admins, systems admins etc. You will find professionals here who are primarily working with appliances or are monitoring data coming out of these security systems. This domain is the widest and covers a broad spectrum of security services. Think of a Security operations centre carrying out day to day tasks keeping the systems uptime, managing firewall policy, looking at the alerts from these systems and initiating the Incident response process etc.
* Anyone starting in this domain will have real indepth knowledge of Security operations and will have the confidence and experience to excel into other domains.

Targeted Positions

- Network Security Engineers
  - Firewalls, Proxies, email gateways
- IAM administrator
- Endpoint Admins : EDR systems management
- SIEM, SOAR, TIP admins
- Security Analysts, Incident response, Forensics engineers

Certifications

- Security +
- Network +
- CCNA Security
- CCNP. CCIE Security
- Leading Certification for Firewalls, EDR (Carbon Black, Fidelis, NBA etc
- Splunk Admin, ArcSight Admin
- Security Analyst and IR certifications https://www.sans.org/cyber-security-skills-roadmap/#

Institutions/Organizations

- https://www.comptia.org/
- https://www.isaca.org/
- www.eccouncil.org
- www.sans.org

If you like:

- Roles that highly intensive and very hands on
- Device management and playing with technology
- Operations roles where you get you hands dirty.

Pre-Requisites

- Basic Security and fundamentals
- Product level certifications like CCNP, CCNA etc.

VERIFIERS

Description

Verifiers are the experts who validate the implemented controls. These controls could be technical nature or of process. Successful people in this domain are intuitive in nature and problem/puzzle solvers. One needs to be always thinking out of the box and trying new techniques, practice to test a code or alternate ways to pass through security defence systems. Some approach applies for non technical roles where implemented process in place requires critical review of how an organisations internal process can impact the privacy and integrity of the organisation

Targeted Positions

- Penetration Tester
- Red/Purple Teamers
- IT security Audit

Certifications

- OSCP (PWK) https://www.offensive-security.com/
- CEH https://www.eccouncil.org/ethical-hacking/
- CISA https://www.isaca.org/credentialing/certifications
- CDPSE https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer

Institutions/Organisations

- https://www.offensive-security.com/
- https://www.isaca.org/
- www.eccouncil.org
- www.sans.org
- https://attack.mitre.org/

If you like:

- Roles that require extreme technical and niche skills
- Continuously enhance your skill set and learn/develop new attack techniques
- To belong to a cool and rebellious group of professions ;)

Pre-Requisites

- Exceptional grasp of the Cybersecurity concepts
- Quick learner
- Well versed with Linux systems and Operating systems in general
- Very good network fundamentals

THINKERS

Description

Thinker are the people who have a more pragmatic approach on how Cyber Security functions in an organisation. They are the people who develop the strategy, alignment with the business and set the do's and don'ts of the organisation.

Targeted Positions

- CISO
- Security Governance officer
- Governance Risk and Compliance (GRC) officers
- Policy makers
- Security Consulting
- Business Continuity and Disaster Recovery roles

Certifications

- CISM https://www.isaca.org/credentialing/cgeit
- CGEIT https://www.isaca.org/credentialing/cism
- CRISC https://www.isaca.org/credentialing/crisc
- CISSP https://www.isc2.org/Certifications/CISSP

Institutions/Organisations

- https://www.isc2.org/
- www.isaca.org
- www.eccouncil.org
- www.sans.org
- https://attack.mitre.org/

If you like:

- Roles with critical thinking
- Developing and leading programs.
- Would like to engage more with business side of Security services
- Manage security metrics and performance indicators
- Policy making and execution
- Risk and compliance Management

Pre-Requisites

- 5+ years of relevant experience
- Bachelors degree in relevant field


CISCO