الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies

Cybersecurity Quarterly Bulletin

Q2 2020

Classification: Open
TLP: White

Contents

Highlights from the Quarter

Q2 2020 (April-June)

The implications of the global pandemic are still the macro factor affecting the cybersecurity industry recently; however, the quarter has also been marked by a number of key cybersecurity events.

Key highlights include the International Institute for Management Development's release of the 2020 World Competitiveness Ranking, in which Saudi Arabia ranked 2nd for 'constant development of cybersecurity for institutions'.

Artificial intelligence (AI) and quantum computing are highlighted as technologies that can improve cybersecurity.

Bits and Bytes

Key quarterly statistics, top threats and targeted sectors globally

+ 38 billion

Devices connected to the internet by 2020[1]
The expected growth is 28.7% CAGR over the 2018-2025 period, which will widen the attack surface available for exploitation.

#1 motive

Financial gain behind attacks on healthcare [2]
88% of the attacks against the healthcare sector are motivated by financial gain, while 12% are motivated by fun or convenience.

+50%

Increase in data breaches caused by human mistakes from 2019-20[2]
This significant growth of human errors accounts for approximately 17% of data breaches globally.

74%

Organizations considering permanent remote working for at least part of their workforce[3]
On average, 5% of the workforce per company may move to permanent remote working. Cybersecurity will play a major role in this transition.

Top 5 targeted sectors globally in Q2 2020*

01	Public	17%
02	Science and Technical	13%
03	Healthcare	12%
04	Finance	11%
05	Education	8%

Top 5 global threats in Q2 2020*

01	Malware	42%
02	Account Hijacking	21%
03	Targeted Attack	11%
04	Vulnerability	5%
05	Malicious Script Injections	3%

Top 5 threats in KSA in Q2 2020**

01	Malware
02	Penetration/attempt to penetrate
03	Unauthorized access/attempts of
04	Data leakage
05	Reconnaissance Attack

[1] IBM Security, X-Force Threat Intelligence Index 2020, February 2020.
[2] Verizon, 2020 Data Breach Investigation Report.
[3] Gartner, Press Release: Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently, April 2020.

* Numbers show the distribution (%) over the total number of attacks registered worldwide for Q2.
**NCA analysis. Numbers show the top cybersecurity threats registered in the Kingdom of Saudi Arabia for Q2.

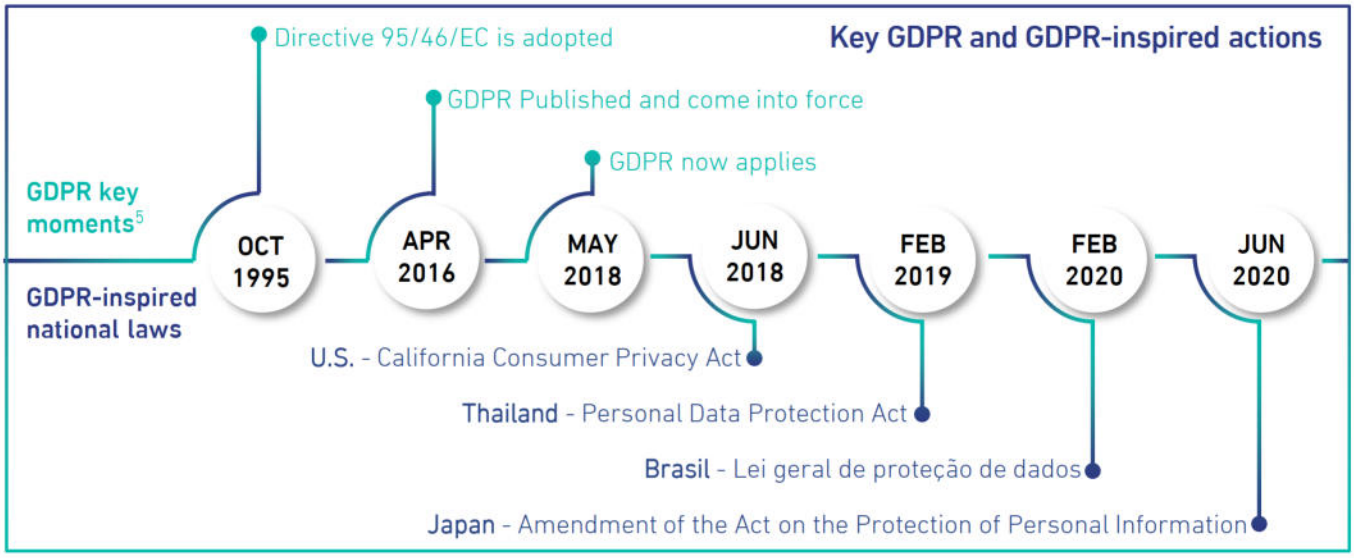
Global Cyber Outlook

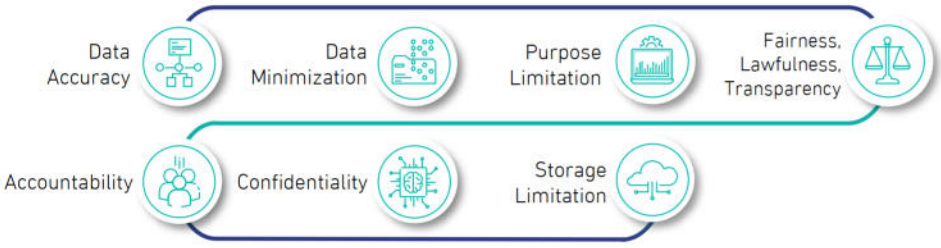
Cybersecurity headlines from around the world

Two years later: how the global privacy landscape changed with GDPR

May 2020 marked the second anniversary since the EU GDPR came into force. It was introduced to regulate how organizations should manage and protect users' data and to pave the way for a European Single Digital Market.

The GDPR not only shaped European data protection, but has also become a global standard, inspiring the "California Consumer Privacy Act", the Brazilian "Lei geral de proteção de dados" and the "Act on the Protection of Personal Information" in Japan.[4]



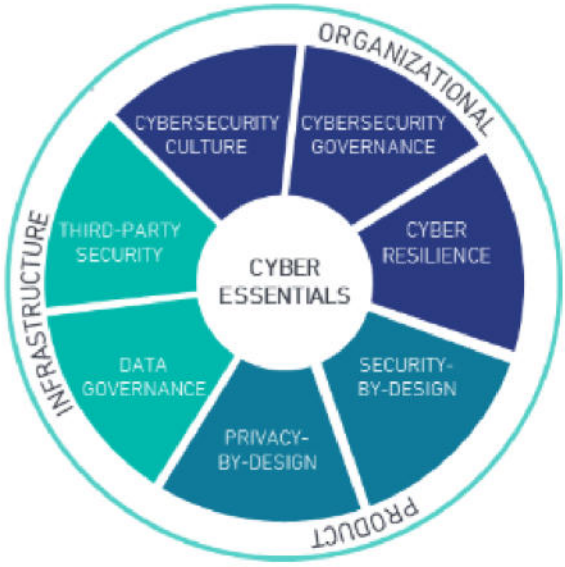


Given the relevance of the GDPR, NCA has published a guide based on seven pillars to help Saudi organizations determine the extent of its applicability, and to help them better handle its provisions.[6]

World Economic Forum released a Cybersecurity Framework for investors and entrepreneurs

According to a report from the World Economic Forum (WEF), cybersecurity suffers from an imbalance between the "time to market" and "time to security", as companies are expected to release new technologies at a fast pace.

The report notes that this pitfall can be avoided by adopting a "secure by design" approach focused on embedding cybersecurity in products and services from their development phases. To this end, the report includes a framework to help investors and entrepreneurs - working in this fast-paced scenario - implement cybersecurity in their products and services. The document also contains a set of cyber essentials that stakeholders can adopt to improve security.[7]



[4] The New York Times, G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog, June 2018.

[5] European Data Protection Supervisor, The History of the General Data Protection Regulation. European Commission.

[6] NCA Guidelines for GDPR

[7] World Economic Forum, Incentivizing Responsible and Secure Innovation: A framework for investors and entrepreneurs, June 2020.

National Cyber Outlook

Cybersecurity headlines regarding the Kingdom of Saudi Arabia

NCA released cybersecurity controls for remote working

As a result of the COVID19 pandemic, remote working has increased dramatically around the globe. This change has happened in the Kingdom as well, prompting new considerations around cybersecurity.

In response, NCA has issued dedicated controls, built around eight steps to help users maintain cybersecurity while working remotely.[8]

NCA steps for secure remote working

2020 World Competitiveness Ranking: Saudi Arabia ranked 2nd in Cybersecurity

The Institute for Management Development (IMD) recently released the 2020 World Competitiveness Ranking, which assesses 60+ countries on aspects of competitiveness including cybersecurity. This year KSA ranked 2nd for 'constant development in cybersecurity for institutions'.[9]

This recognition confirms the role of KSA in cybersecurity at the international level, and demonstrates the commitment of the Saudi Government to improve national cybersecurity. To this end, and to support the Country's 2030 Vision, the Kingdom implemented reforms, initiatives and programmes concerning cybersecurity. This has been made possible by support from Saudi leadership and by the efforts of the National Cybersecurity Authority.

The NCA has worked to implement cybersecurity policies, governance mechanisms, structures, standards, controls and guidelines, which have been circulated among interested entities inside and outside of Saudi Arabia.

The NCA will continue on this path with the goals of strengthening Saudi Arabia's cybersecurity posture for the benefit of citizens and organizations around the country.[10]

[8] CERT.SA, Remote Working Guide, 2020.
[9] IMD World Competitiveness ranking 2020, 2020
[10] NCA News, The Kingdom Places Second for Constant Development on the Cybersecurity Index for Institutions, on the Global Competitiveness Report, June 2020.

Top Security Stories

A look at prominent cybersecurity events from the last quarter

Web Services hit by record-sized DDoS[11]

Location: Worldwide

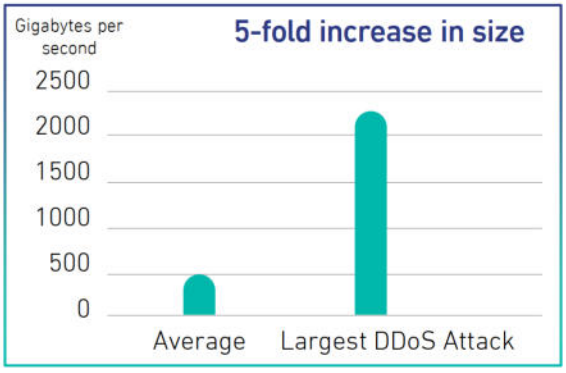
Sector: Web / Cloud Services

Date of disclosure: 13th June 2020

Type of attack: Distributed Denial of Service (DDoS)

Description: Amazon Web Services (AWS) was the victim of a three-day 2.3 Terabytes per second DDoS attack in February. This was the largest DDoS attack ever recorded.

On average, DDoS attacks peak at 500 Gigabytes per second, and this attack was almost five times larger. The motivations for the attack are unknown, but the method appears to be a new kind of DDoS "reflection attack". This technique makes DDoS attacks more efficient and less likely to be blocked by traditional anti-DDoS security measures.



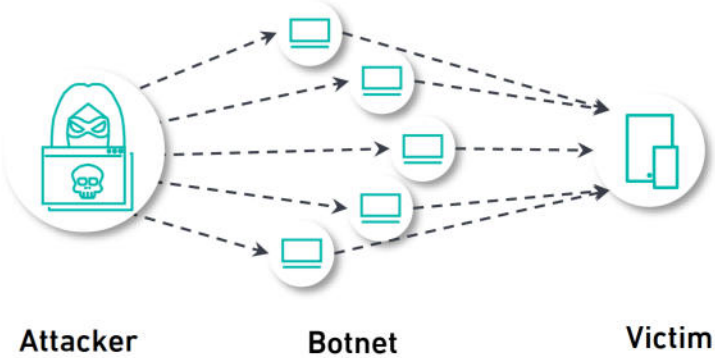
Impact: The attack was 44% larger than similar previous attacks. The incident was disclosed several months after it happened.

Lessons learned: The incident demonstrated it is possible to be a target for extremely large DDoS attacks. Key recommendations to mitigate the impact : First, design your network in order to avoid "single points of failure", and segregate it in a way that protects the most vital parts from outside traffic. Then ensure full and real-time visibility of your network, and implement alerting systems in case network traffic grows beyond certain thresholds.

About a DDoS attack

DDoS takes advantage of the limited data capacity of networks. Attackers flood the target with a large amount of data and, when network capacity is exceeded, hosted services are likely to be negatively impacted or rendered unavailable.

In order to send this large volume of data, attackers use previously infected devices called bots, which are controlled by the attacker. Collectively, these are called a botnet, and are used to generate the traffic necessary to overwhelm the victim.[12]



[11] AWS Shield, Threat Landscape Report – Q1 2020.

[12] Kaspersky, What is a DDoS Attack? - DDoS Meaning.

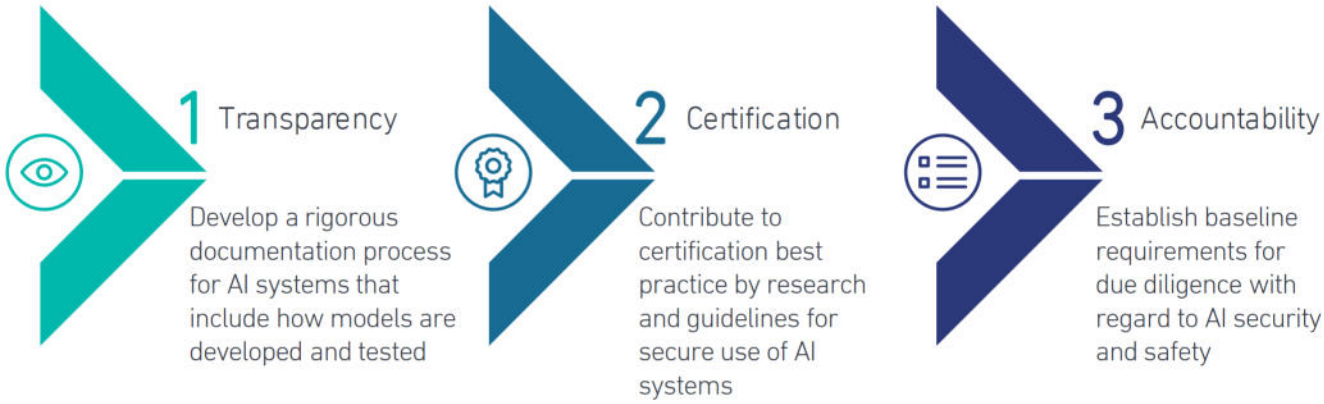
Cyber Secure

Useful cybersecurity tips for safe implementation of Artificial Intelligence (AI) technologies

Artificial intelligence is beginning to play a key role in organisational transformation.[13] Indeed, artificial intelligence opens up new opportunities and new capabilities. Organizations should endeavour to understand the applications, and cybersecurity recommendations for secure AI implementation.

Embracing the future of AI - securely

The proliferation of AI systems in key sectors—including transportation, health, Financial, and other sectors— highlights the importance to ensure the cybersecurity of these systems. This will require to understand how AI systems can be secured through a combination of transparency guidelines, certification , and accountability measures.[14]



Tips for securely developing and deploying AI

Understand user and stakeholder needs. Given its cybersecurity requirements, it is paramount to adopt AI with clear use cases that have been identified.

Develop and enhance forensic capabilities. AI transparency and accountability are essential to maintain cybersecurity, build public trust in the deployment of this emerging technology.

Retain oversight. Cybersecurity professionals to support with a clear and nuanced understanding of AI.

Examine the code. When developing AI technologies, the relevant code and algorithms should be examined by cybersecurity experts.

Monitor the threat landscape. AI technology would be used by threat actors to automate attacks against organizations. It is advisable to understand how AI is being exploited by attackers, in order to best protect organizations from such threats.

[13] World Economic Forum, AI Government Procurement Guidelines, September 2019.

[14] How to improve cybersecurity for artificial intelligence, Brookings, 2020.

Looking Ahead: New Trends

A look at the latest AI-related trends and how they are influencing cybersecurity

How AI can enhance cybersecurity[15]

Just as AI systems need innovative cybersecurity tools and methods to improve their trustworthiness and resiliency; in parallel cybersecurity can use AI to increase its effectiveness.[16] There are several key avenues where AI can be used to strengthen cybersecurity:

Although AI is still in its infancy, and expected to grow significantly, it is already a reality for many organizations. According to surveys, more than 70% employ AI in one or more areas of cybersecurity, with Network Security the most common application.[17]

Learning

AI uses a vast amount of structured and unstructured data. Through machine learning and deep learning, AI can be used to better understand cybersecurity threats and risk.

Reasoning

AI uses reasoning to recognize links between different threats (e.g. malicious files, suspicious IP addresses, etc.). This allows cybersecurity experts to dramatically increase their threat response time.

Augmenting

AI brings dramatic efficiency and improves accuracy to labor-intensive human tasks, reducing the amount of time needed to identify and analyze threats, and launch a coordinated response.

AI defense: cybersecurity use cases[18]

The cybersecurity industry has already started to use AI capabilities to defend networks and systems, with key activities including:

- Enhanced monitoring and analysis of network traffic.
- Augmented security analysis.
- Threat prediction and real-time threat detection.
- Enabling auto-response and threat mitigation.

AI as a cyber threat: deepfakes

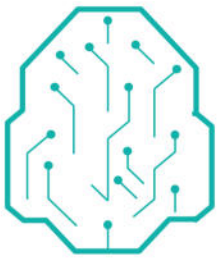
AI is effective at generating false audio and video content. Malicious actors then use this content — known as deepfakes — to discredit and extort victims, forcing them to pay ransoms in exchange for content removal. Deepfakes are also deployed in disinformation campaigns.[19]

[15] IBM, Artificial intelligence for a smarter kind of cybersecurity.
[16] NITRD, Artificial Intelligence And Cybersecurity: Opportunities And Challenges, Technical Workshop Summary Report, March 2020.
[17] Velocity Global, How Are Global Businesses Utilizing AI?, January 2019.
[18] Built in, 30 companies merging ai and cybersecurity to keep us safe and sound, March 2020.
[19] Technology Innovation Management Review, The Emergence of Deepfake Technology: A Review, November 2019.

Spotlight on Cyber Innovation

Quantum computing and the latest innovation in the cybersecurity field

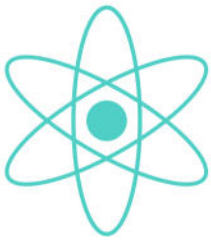
Despite dating back 30 years, the term "quantum computing" is now getting mainstream attention. Traditional computing devices (such as laptops and smartphones) use binary digits, or bits, for their operations. These bits can only assume a value of 0 or 1. However, in quantum computing, the basic unit is the qubit, which can assume a value of 0 and 1 at the same time. This allows quantum computers to operate at speeds exponentially faster than traditional ones, and opens new possibilities for previously-impossible computing tasks.



In a recent experiment, a quantum computer performed a three-minute calculation that, according to some estimates, would have taken 10,000 years for a system with the computational power of 100,000 traditional desktop computers.[20] Such computational power could bring about huge changes for cybersecurity, particularly with cryptography. According to researchers, quantum computing will make it possible to quickly break widely adopted algorithms. For instance, a recent study tested the 2048-bit RSA algorithm, and concluded it could be broken in eight hours using quantum computing.[21]

Researchers are working to prepare cybersecurity for the quantum age. For example, the US National Institute of Standards and Technology (NIST) shortlisted 26 algorithms to be tested, hoping to find some "quantum resistant" algorithms among this selection.

Another approach - called Sovereign Encryption – advocates for national entities to deploy multiple algorithms, for example, one algorithm for financial services hosted on national servers, and a different one for national healthcare services. This use of multiple algorithms poses a risk that they may be less rigorously tested and may contain vulnerabilities. However, the use of so many of them helps to avoid the risk of single points of failure (e.g. when widely adopted algorithms are broken).



There is no scientific consensus about the time required to construct useful quantum technology computers. While the most optimistic experts estimate this may take 5-10 years, more cautious (and arguably more widely held) estimates predict 20-30 years.[22] However, organizations are advised to get quantum-ready now. This is likely to be a long process that could take decades for the most complex organizations – such as large corporate or national entities – to complete.

Prepare for quantum computing

Stronger data protection is essential. Encryption alone is not enough, and data should be made inaccessible to unauthorized parties, as attackers could resort to "harvest and decrypt" techniques, which focus on gaining access to encrypted data, and storing it until it can be decrypted with quantum computers.[23]

Organizations should prepare for quantum computing with "crypto agility," which means the ability to continuously update cryptographic protection and algorithms in order to stay ahead of attackers.[24] As part of this, it will be essential to regularly research and develop quantum-resistant cryptographic algorithms.[25]

[20] Nature, Hello quantum world! Google publishes landmark quantum supremacy claim, October 2019.
[21] Craig Gidney et al., How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits , December 2019.
[22] Spectrum, The Case Against Quantum Computing, November 2018.
[23] Deloitte, Technology, Media, Telecommunication Predictions, 2019.
[24] National Institute of Standards and Technology , Report on Post Quantum Cryptography, April 2016.
[25] Quantum Safe Cryptography (QSC), European Telecommunications Standards Institute, ETSI White Paper No. 8, June 2015.

This quarterly bulletin has been compiled by the National Cybersecurity Authority (NCA) of the Kingdom of Saudi Arabia (KSA). Its goals are to provide readers with an overview of the most important cybersecurity events and data from the quarter and to highlight the most interesting facts related to the focus of this issue. Aiming to :

- Elevate Cybersecurity knowledge and capabilities
- Provide outlook on latest cybersecurity trends, threats & risks

This report contains the information from several parties and individuals, noting that all information included in the report is indicative only. Also, the NCA does not bear any responsibility - under any circumstances - towards any party as a result of any decision or action taken or will be taken by that party based on the content of this report. The NCA asserts that it is not completely or partially responsible for any direct or indirect prejudice may occur.

About the NCA

The National Cybersecurity Authority (NCA) was established in 2017. The NCA is the government entity in charge of cybersecurity in Saudi Arabia and it serves as the national authority on all related affairs. It has both regulatory and operational functions related to cybersecurity and works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities

https://nca.gov.sa @NCA_KSA