الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Cybersecurity Quarterly Bulletin

Q4 2020

Classification: Public
TLP: White


698.11
226.34

Contents

Highlights from the Quarter

Q4 2020 (October - December)

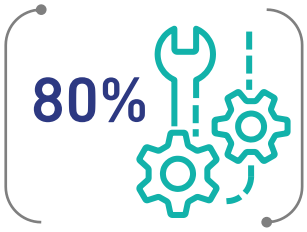
2020 was a year unlike any other in living memory. The COVID-19 pandemic cast a long shadow over the world and impacted every aspect of society. Cybersecurity was no exception. This Bulletin and previous editions examine the influences of the pandemic on cybersecurity, and the readiness and resilience of governments and the private sector. 2020 was filled with many incidents, including notable attacks on healthcare infrastructure as well as the Solarwinds incident at the end of the year, which clearly demonstrated the far-reaching implications of a compromise in a critical software supply chain. 2021 will doubtless see its share of high-profile cybersecurity threats, but it's clear that the highlights of previous years tend to offer little insight into the challenges of the coming year. Every year is different in its own way. Preparedness and resilience are the most valuable attributes to bring into the New Year.

Bits and Bytes

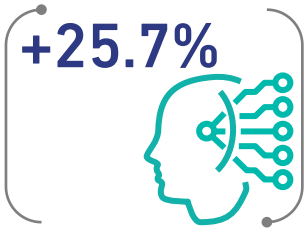
Key cybersecurity statistics and predictions

The global cyber insurance market is predicted to triple by 2025[1]
The major factor is the increasing number of cyber attacks and incidents.

The global automotive cybersecurity market is predicted to double by 2025[2]
It is key to secure information exchange between vehicles and their surroundings.

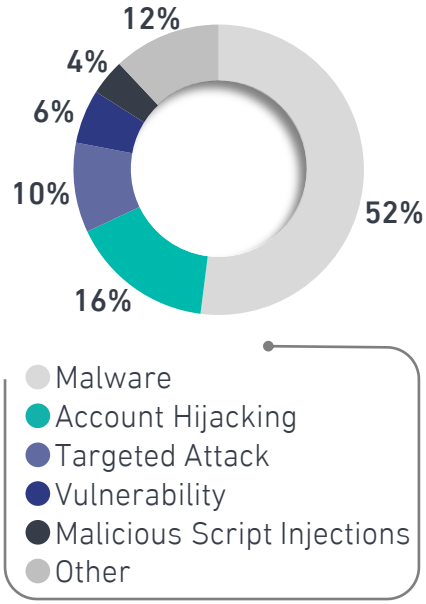


Of companies re-structured their cybersecurity infrastructure due to COVID-19[3]
This change has been led by large-scale enterprises.



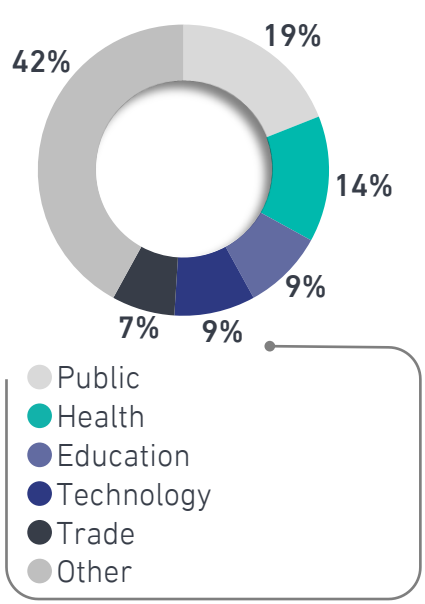
Dramatic AI cybersecurity market growth in next ten years[4]
Forecast to grow at a 25.7% CAGR from 2020-2030.

Top 5 global threats in Q4 2020 *



Top 5 threats in KSA in Q4 2020 **

Top 5 targeted sectors globally in Q4 2020 *



* Numbers show the distribution (%) over the total number of attacks registered worldwide for Q4.

**NCA analysis. Numbers show the top cybersecurity threats registered in the Kingdom of Saudi Arabia for Q4.

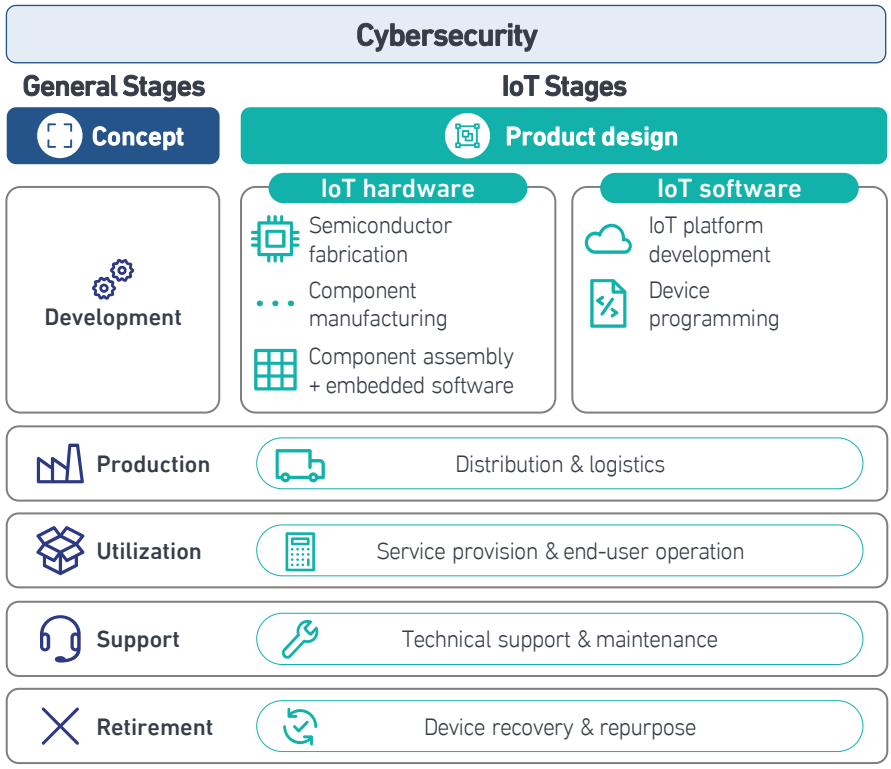
Global Cyber Outlook

Cybersecurity headlines from around the world

Securing the IoT supply chain

The US Internet of Things Cybersecurity Improvement Act (signed into law in December 2020) tasked the National Institute of Standards and Technology (NIST) with developing minimum cybersecurity standards and guidelines for IoT devices.[5] Although this law only applies to devices procured by the US government, it may motivate vendors to improve cybersecurity across the IoT supply chain.[6]

The European Union Agency for Cybersecurity (ENISA) also released guidelines for securing the IoT supply chain (see reference model on the right), which can serve as a blueprint for IoT standards to be developed in 2021.[7]



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Cloud Cybersecurity Controls[8]

This sets cybersecurity requirements for cloud computing from the perspective of cloud service providers and cloud service tenants.

Cybersecurity professionals stand up to the pandemic

Despite a global shortage of cybersecurity professionals, several organizations' current cybersecurity personnel successfully faced many of the challenges posed by the COVID-19 pandemic.[9] The NCA recognizes these professionals' critical role and has adopted several measures to equip Saudi professionals with the cybersecurity skills to qualify them for the labor market.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Saudi Cybersecurity Higher Education Framework (SCyber-Edu)[10]

A reference guide for the development of cybersecurity higher education programs

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

CyberPro+ in cooperation with HRDF and SITE[11]

500 graduates undergo cybersecurity training for 6 months

(ISC)² Cybersecurity Workforce Study Findings[12]

92% cybersecurity professionals prepared for the remote work shift

54% concerned about personnel spending in 2021

3.1 Million global cybersecurity workforce gap

+89% believe that the global cybersec workforce needs to increase in future

56% of surveyed organizations believe that the cybersecurity staff shortage represents a risk

Saudi Cyber Outlook

The Saudi Model for Strengthening Cyber Resilience During the Kingdom's G20 Presidency Year

Strengthening the Cyber Resilience during G20 Presidency

For the first time in history, the G20 Presidency was a wholly digital experience. This had an impact on the cyber threat landscape facing the G20 and elevated the importance of cybersecurity during the Kingdom of Saudi Arabia's G20 Presidency year.

The NCA worked on strengthening the cyber resilience throughout the G20 Presidency year, including the Leaders' Virtual Summit.

G20 Cybersecurity Resilience in Numbers

Program Governance

400+
Cybersecurity Specialists Participated in the program

350+
Entities' cyber readiness were elevated

450+
Reports were released

400+
Days of preparation and execution

Cybersecurity Assessments

120+
Cybersecurity assessments conducted, including:

1. Risk Assessment
2. Penetration Testing & Vulnerability Assessment
3. Configuration & Architecture review
4. Compromise Assessment
5. Business Continuity Assessment
6. Compliance Assessment
7. User Access Review

100+
Entities were assessed

Cybersecurity Operations

600+
Cybersecurity Warnings shared with related entities

10K+
Hours of continuous Cybersecurity Monitoring

Cybersecurity Awareness and Cyber Drills

100
Entities Participated in cyber drills

9
Cyber Drills were conducted for related entities

60+
Workshops conducted for related entities, with participation of the Chief Information Security Officers

Top Cybersecurity Stories

SolarWinds[13]

Location: United States

Sector: IT

Date of disclosure: 13 Dec 2020

Type of attack: Compromised software update

Description

US-based software provider SolarWinds was the victim of an attack in spring 2020. The attackers breached the SolarWinds' network and inserted malware in updates for Orion, a software application for IT inventory management and monitoring. These compromised updates were available from March - June 2020 and are believed to have been installed by at least 18,000 SolarWinds customers, including government, technology, and telecom organizations across North America, Europe, Asia, and the Middle East.

Impact

Cyberespionage is believed to be the primary motivation, particularly against the US government.[14] A joint statement by the four US agencies in charge of intelligence and cybersecurity said that the government has so far identified fewer than 10 federal agencies whose internal computer systems had been infiltrated in the hack.

Lesson learned

Widely used software can serve as a single point of entry into thousands of organizations, and it requires close and sustained security attention. This incident raises the importance of the cybersecurity of the supply chain for information and communications technology.

FireEye[15]

Location: United States

Sector: Cybersecurity

Date of disclosure: 8 Dec 2020

Type of attack: Compromised software update (see above)

Description

Attackers compromised a SolarWinds software update (see above) and used it to gain entry into the networks of US-based cybersecurity company FireEye.[16] The attackers used this access to obtain FireEye's 'red team' tools, which are programs that replicate sophisticated hacking tools and are used to look for network vulnerabilities. Although these 'red team' tools did not include zero-day exploits, attackers could still use them to conceal evidence of cyber attacks and hamper forensic investigations.

Impact

Although the attacker had access to FireEye's internal system, there is no evidence that the attacker had access to customer information. Also, there has been no evidence that attackers have used the stolen 'red team' tools to date. However, attackers could still exploit such tools to increase their offensive capability.

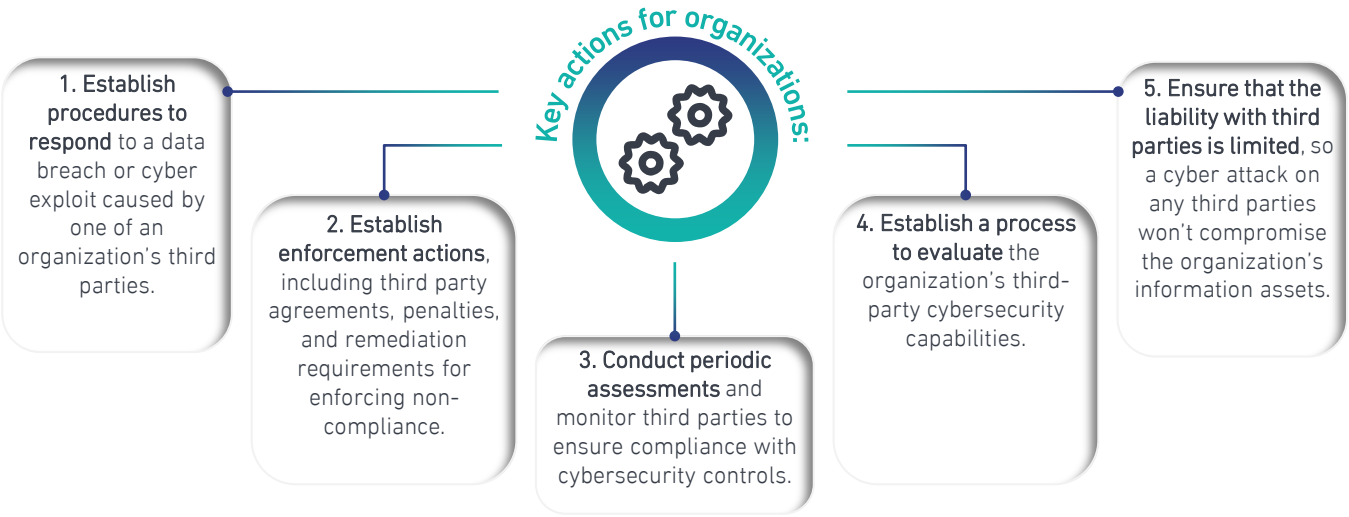
Lesson learned

This incident highlights the effectiveness of patient and well-resourced attackers.

Cyber Secure

There are many challenges in managing cybersecurity risks from external parties

According to Ponemon's report, in the past two years, 82% of organizations surveyed experienced a third-party data breach, costing an average of $7.5 million to lessen the impact.[17] These defects cover five main areas: laptop (including desktop) and server protection, virtualization protection (on premises or cloud-based), data at rest, and in motion protection. Major related risks are ransomware attacks, website defacement, data modification, and malicious use of PII.[18]

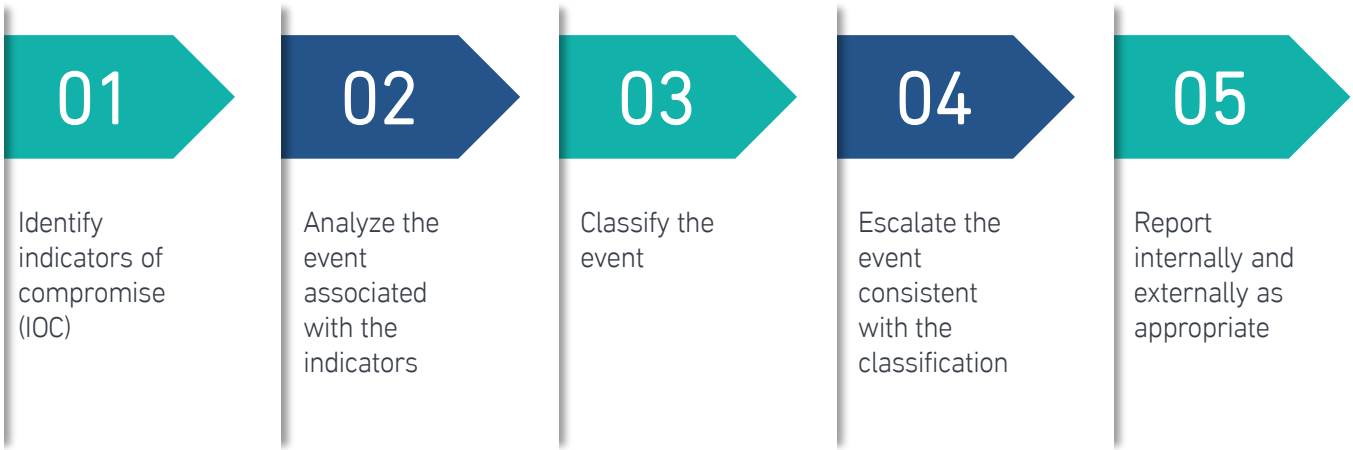


NCA's Essential Cybersecurity Controls include cybersecurity requirements to secure national organizations against third-party risks (ECC – 1: 2018, control no. 4-1).[19]

Building an Incident Identification and Assessment Process: Key Pillars[20]

Incident identification is becoming a key component of risk management. The two main factors to conduct an incident identification are the indicators (external or internal the organizations) and an accurate analysis conducted by experts in the field.

In order to build an effective incident identification and assessment, organizations need an accurate and comprehensive approach based on the following five key pillars:



NCA's Essential Cybersecurity Controls include requirements for cybersecurity incidents reporting to NCA, sharing incidents notifications, threat intelligence, breach indicators and reports with NCA (ECC – 1: 2018, control no. 2-13-3).[21]

Looking Ahead: New Trends

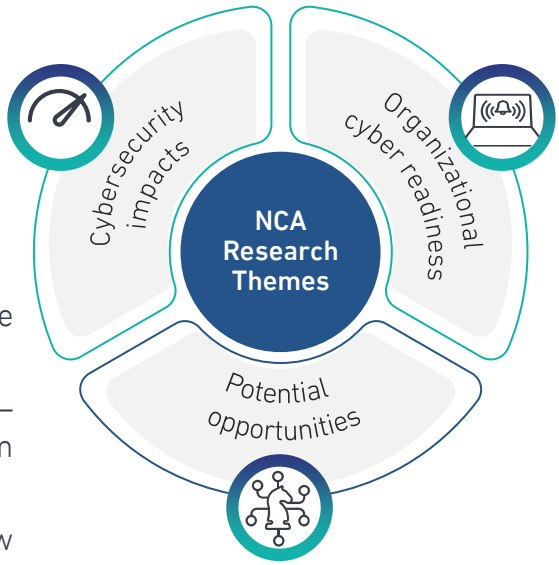
Preparing for the future: how to manage new evolving cyber risks

A new research on the cybersecurity impacts of the COVID-19 pandemic

The COVID-19 pandemic has touched every corner of the globe and as it unfolded and the effects became clearer, it has become equally clear that robust cybersecurity is essential to manage the impacts of the pandemic, establish a firm foundation for economic recovery and growth, and make investments that will last beyond this crisis.

The National Cybersecurity Authority (NCA) research finds that:

1. With the increase in remote working, the attack surface available to threat actors has created new opportunities.
2. Limited cybersecurity expertise is presenting challenges – both for short-term staffing and for the longer-term development of cybersecurity professionals.
3. High levels of stress and uncertainty are offering new opportunities for phishing and ransomware.



How to manage cyber risk from emerging technologies

Changes in the technology landscape pose significant cybersecurity risks. In its new report, the World Economic Forum discussed the measures needed to tackle systemic risks inherent in emerging technologies, with a particular focus on ubiquitous connectivity, artificial intelligence, quantum computing, and digital identity.[22]

Emerging Tech	Ubiquitous Connectivity	Artificial Intelligence	Quantum Computing	Digital Identity
Cybersecurity Measures	Identify and classify the **critical infrastructure** for the operation of multiple services	Invest in **AI-enabled defenses** to predict cyber threat and attack strategies	Develop **sovereign quantum capability** through public-private partnerships	Develop a globally **interoperable governance framework** for digital identity management

A collective approach to effectively manage emerging technologies' cyber risks is imperative. Each stakeholder group has a role to play in managing future cyber risks.

Stakeholders' role in managing future cyber risks

Cybersecurity and Technology Sector
Identify emerging cybersecurity risks and develop interoperable controls

Industry and Government Leadership
Promote cybersecurity standards to strengthen trust and cybersecurity throughout the emerging technology

International Community
Build cybersecurity capacity to reduce cyber threats and enable secure adoption of emerging technologies worldwide

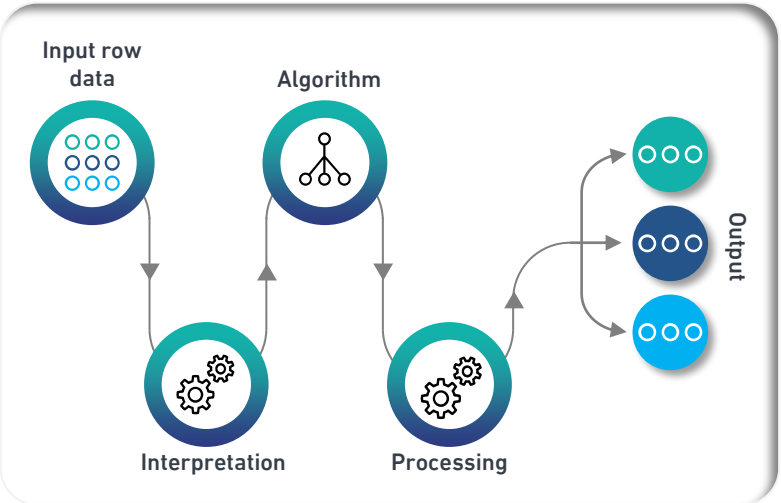
Spotlight on Cyber Innovation

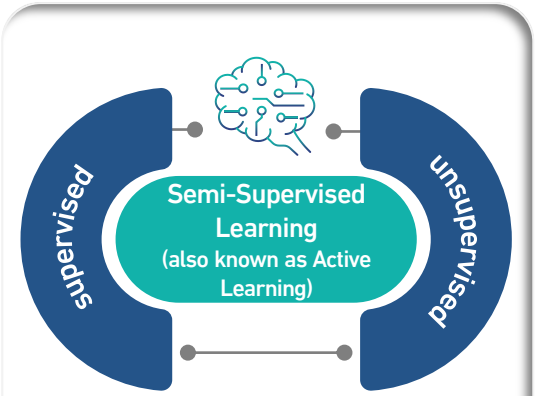
Innovative solutions to cybersecurity challenges are emerging from accelerator programs

Unsupervised Machine Learning: a Cross-Sector Innovation

Machine Learning (ML) includes both supervised and unsupervised learning. The first relies on a human-driven labelling process for capturing information, while the latter captures inferences from datasets without labels or human intervention.

Unsupervised ML is highly valuable in cybersecurity, as it does not look for a specific label, but instead flags as dangerous any pattern that is atypical (and therefore poses a potential threat). A growing number of start-ups are heavily investing in unsupervised ML to detect new cyber attack methods.[23]



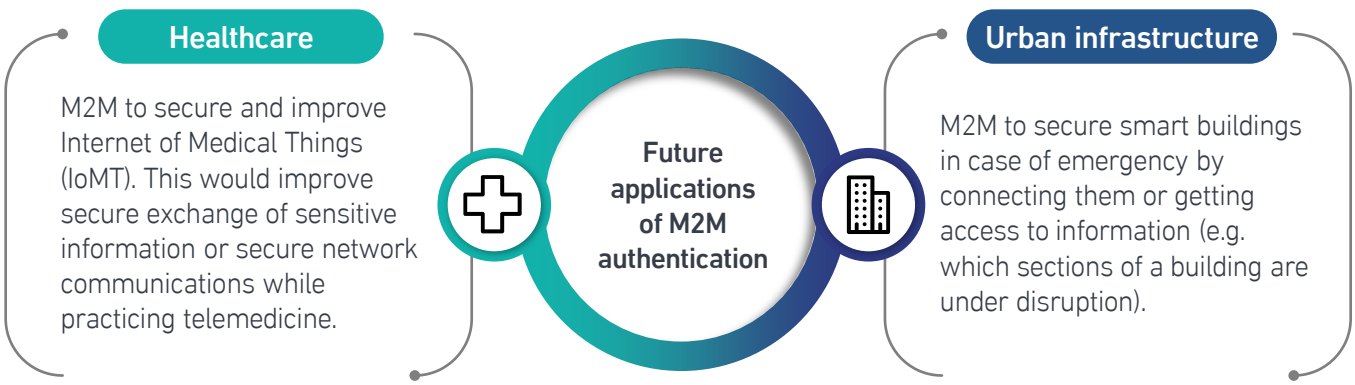


Semi-supervised learning makes predictions on how a network should behave. It looks for abnormal patterns (the same as unsupervised ML); then once it finds abnormal patterns, it labels them as threats (the same as supervised ML).[24]

Machine-to-Machine authentication: A new frontier for secure IoT and network communications

Internet of Things (IoT) and Machine-to-Machine (M2M) technologies are becoming predominant in many sectors, making it essential to increase efficiency by identifying alternatives to traditional cybersecurity authentication technologies (which often require human interaction).[25]

For this reason, companies and governments are investing heavily in M2M authentication. This consists of networks of smart sensors, routers, and an authentication server. These components communicate with each other and are responsible for performing the authentication procedure.[26]



References

[1] https://www.prnewswire.com/news-releases/global-cyber-insurance-solutions-analytics--cybersecurity-and-services-market-2020-2025-key-players-are-allianz-aig-chubb-aon-zurich-axa-and-berkshire-hathaway-301166366.html

[2] https://www.prnewswire.com/news-releases/automotive-cybersecurity-market-by-form-security-application-vehicle-type-ev-type-and-region---global-forecast-to-2025-301167143.html

[3] https://www.hackread.com/companies-re-structured-cybersecurity-infrastructure-2020/?web_view=true

[4] https://www.researchandmarkets.com/reports/5184623/ai-in-cyber-security-market-research-report-by?

[5] https://www.govtrack.us/congress/bills/116/hr1668

[6] https://www.helpnetsecurity.com/2020/10/29/iot-cybersecurity-improvement-act-of-2020/?web_view=true

[7] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[8] https://nca.gov.sa/en/pages/ccc.html

[9] https://www.isc2.org/Research/Workforce-Study

[10] https://nca.gov.sa/en/pages/news/news44.html

[11] https://nca.gov.sa/en/pages/news/news42.html

[12] https://www.isc2.org/Research/Workforce-Study

[13] https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

[14] https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8

[15] https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

[16] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[17] https://www.cybergrx.com/resources/research-and-insights/ebooks-and-reports/the-cost-of-third-party-cybersecurity-risk-management

[18] https://www.helpnetsecurity.com/2020/11/25/combating-third-party-cyber-risk/?web_view=true

[19] https://nca.gov.sa/files/ecc-en.pdf

[20] https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiic-incident-identification-and-assessment.aspx

[21] https://nca.gov.sa/files/ecc-en.pdf

[22] https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

[23] https://www.ibm.com/cloud/learn/unsupervised-learning

[24] https://www.technative.io/why-unsupervised-machine-learning-is-the-future-of-cybersecurity/

[25] https://www.researchgate.net/publication/319024120_A_Lightweight_Authentication_Mechanism_for_M2M

[26] https://eprint.iacr.org/2018/891.pdf

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. It aims to:

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

This report contains 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 that 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 that 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