G20
SAUDI ARABIA 2020

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

SITE
الشركة السعودية لتقنية المعلومات
Saudi Information Technology Company

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

2021

Classification: Open
TLP: White

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Since its inception, The National Cybersecurity Authority (NCA) works closely with public and private entities and international partners to improve cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-prority sectors, and government services and activities in alignment with Vision 2030. "A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity" is the strategic vision developed by NCA to reflect the strategic ambition of the Kingdom in a manner that balances between security, trust and growth. This report highlights the efforts to secure stakeholders and assets invloved in G20 events throughout the G20 Presidency, leading up to the leaders' Virtual Summit. We take this opportunity to extend our sincere gratitude to the Ministry of Communications and Information Technology (MCIT), Saudi Data and Artificial Intelligence Authority (SDAIA), G20 Saudi Secretariat (G20SS), Saudi Information Technology Company (SITE), and STC for their contribution in raising the level of readiness and resilience of the Saudi cyber space during the G20 Presidency.

Content

Executive Summary

In today's digital world, cybersecurity is becoming an urgent imperative that needs our immediate attention. Due to the COVID-19 pandemic, most events were held online during Saudi Arabia's G20 Presidency year, which changed the threat landscape and introduced new cybersecurity challenges associated with mega events that had to be addressed swiftly.

The G20 is the international forum that brings together the world's major economies. Its members account for more than 80% of world GDP, 75% of global trade and 60% of the population of the planet. Therefore, due to the level and criticality of the participating parties – and the digital nature of communication – ensuring cybersecurity during the G20 Presidency is of high importance.

In 2020, the Kingdom of Saudi Arabia (KSA) held the rotating Presidency of the G20. Due to the fact that cybersecurity is an urgent global challenge, and with the aim to establish international collaboration towards cyber resilience in global economic systems, the G20 Digital Economy Task Force(DETF) introduced a priority titled Security in the Digital Economy, which was aligned with the Presidency year's overall theme and goals.

Moreover, cybersecurity readiness and resilience were essential for a successful Presidency year, especially since most events were held online for the first time ever, due to the COVID-19 pandemic.

Shifting the G20 Presidency to a wholly digital experience changed the threat landscape faced by G20 organizers and introduced new cybersecurity challenges that had to be addressed swiftly.

Saudi Arabia ranked **first** among the Arab states in the Global Cybersecurity Index (GCI) 2020 and **second** globally out of **194** countries.

To address these challenges, Saudi Arabia built on its cybersecurity experience and used international best practices. These efforts were driven by the National Cybersecurity Authority (NCA), the government entity in charge of cybersecurity in Saudi Arabia who developed the G20 Cybersecurity Readiness and Resilience Program.

The Program makes use of a model to secure stakeholders and assets involved in G20 events throughout the G20 Presidency, leading up to the Leaders' Virtual Summit.

While there are some examples of how to secure mega events, there is no recognized methodology or approach that can be drawn from the international stage to effectively secure an event of this caliber. For this reason, designing a model was essential for the NCA's cybersecurity strategy for the G20 Presidency Year.

This report draws upon the NCA's experience in securing the G20 from a cybersecurity perspective in collaboration with its operational arm, the Saudi Information Technology Company(SITE), and other key service providers. Its objective is to provide valuable insight that can be used to benefit future G20 host nations and other mega event organizers.

Principles - The G20 Cybersecurity Readiness and Resilience Program followed a model based on three principles: Inclusiveness, Resilience, and Collaboration.

The Approach - Following a rigorous methodology capitalizing on previous international experiences, the G20

Cybersecurity Readiness and Resilience Program was structured on a two-tier model (Figure 1), with focus on adaptability and continuous improvement.

Tier 1 - aimed to strengthen cybersecurity readiness and resilience throughout the G20 Presidency year:

It focused on codifying roles and responsibilities, identifying information technology assets, and developing specific cybersecurity requirements. This governance structure enabled G20 organizers to assess cybersecurity needs, conduct cybersecurity operations, and strengthen cybersecurity awareness throughout the Presidency year.

Tier 2 - focused on strengthening the cybersecurity readiness and resilience of the Leaders' Virtual Summit:

This event takes place at the end of the Presidency year and was held virtually for the first time. Given the added digital complexity of securing the 2020 G20, the model was tailored to the specific requirements of the Leaders' Virtual Summit. This included new roles and responsibilities and increased cybersecurity capabilities.

Over **120** different cybersecurity assessments were conducted to assess the cybersecurity readiness and resilience throughout the Presidency year.

All information technology and platform assets were closely monitored, and a mitigation plan was enforced to reduce the risk of cyber attacks. A dedicated incident response team was established to complement the efforts of the existing teams.

Finally, several specific cyber drills tailored to the Leaders' Virtual Summit were conducted to prepare and synergize responses to potential cyber attacks.

Each Tier consisted of 4 streams (Figure 1):

Stream 1: Program Governance – Oversight was based on a centralized coordination mechanism that engaged with key stakeholders and monitored the Program's operations.

Roles and responsibilities were identified, codified, and tailored to the specific objectives of the two-tiered approach. The Program's governance structure and oversight mechanisms were comprised of the Executive Committee, the G20 Cybersecurity Readiness and the Resilience Program Team, and the G20 Saudi Secretariat's Cybersecurity Function.

The **G20 Saudi Secretariat's Cybersecurity Function** was responsible for supporting the G20 Saudi Secretariat with executing and facilitating the G20 Cybersecurity Readiness and Resilience Program on a daily basis.

Ultimately, this comprehensive governance structure enabled stakeholders to maximize operational effectiveness while simultaneously coordinating with each team.

Stream 2: Cybersecurity Assessments – These assessments aimed to identify and remediate any risk or

vulnerability in the assets analyzed. They included risk assessments, penetration testing, vulnerability assessments, compromise assessments, compliance assessments, cybersecurity architecture and configuration reviews, and user access reviews. These assessments were conducted by NCA's operational arm, the Saudi Information Technology Company(SITE), and other key service providers.

Stream 3: Cybersecurity Operations – The Program's cybersecurity operations were established and conducted across the two tiers, firstly for the G20 Presidency year, and then enhanced in preparation for the Leaders' Virtual Summit. These operations included threat modeling, cybersecurity monitoring, and incident response (each in continuous evaluation to enhance the cybersecurity readiness and resilience of the overall program).

Stream 4: Cybersecurity Awareness and Cyber Drills – Awareness campaigns, workshops, and training exercises, such as cyber drills, were developed following the two-tiered approach. These activities were tailored for all G20 Saudi Secretariat staff and key stakeholders.

Figure 1.

Lessons Learned

Several lessons and recommendations have emerged from the Saudi G20 Presidency's cybersecurity experience:

Leadership Engagement and Support – Through the mobilization of resources and capabilities, national leadership empowered the G20 Saudi Secretariat. Their support was crucial to ensure the success of the model and the fulfillment of the G20 Cybersecurity Readiness and Resilience Program.

Value of Data, Governance, and Model Design – Data and information on the experiences of previous mega events' hosts should be collected and documented to support further development in the cybersecurity field. Analyzing this data helps identify key areas where additional talent and expertise may be needed. Some of this expertise can come from establishing a team of national and international stakeholders – including third parties – and defining their roles and responsibilities to create synergies across various domains. For example, by creating a Cybersecurity Function within the G20 Secretariat and ensuring that cybersecurity will play a key role at the management and operational levels, the Saudi G20 model can serve as a reference for future G20 Presidencies.

Need for Agility and Coordination with Partners – Unforeseeable adverse events can occur, and this possibility should be factored into the design of a resilient model. Agility is required to swiftly involve new stakeholders, make executive decisions in a timely manner and increase capacity and monitoring of cybersecurity capabilities.

Early Preparation and Scalable Efforts – Cybersecurity efforts should

be appropriate to secure each component of the G20, given the multitude of meetings, events, and workshops occurring throughout the year. Increased coordination efforts by the Secretariat are essential to ensure a homogeneous and sustainable approach to cybersecurity. Incident response teams should be created for the G20 as a whole but should particularly focus on crucial events, such as the Leaders' Summit. Scaling up the incident response capabilities gives these teams the ability to respond to multiple incidents at the same time. It is best practice to start by building on existing plans, capabilities, and methodologies, as these can often be tailored and enhanced to fit specific circumstances.

Scope Management – Identifying direct and indirect stakeholders is a primary step to secure a mega event. This includes both information technology and event assets, whose ownership should be clearly identified to ensure that stakeholders understand their roles and responsibilities. A focused and layered approach was used to monitor and protect the G20 Saudi Secretariat. External dependencies, third parties, and supply chains beyond the Secretariat should also be identified, regardless of their geographical locations. Given that cybersecurity capabilities and skills can vary across the different entities involved in the larger G20 ecosystem, entities' cybersecurity maturity and infrastructure protection levels need to be considered. These entities' different cybersecurity maturity levels can be addressed through mitigation actions and capability reinforcement.

Importance of Regular Cybersecurity Assessments – Through regular assessments, the professionals responsible for G20 cybersecurity can promptly identify assets' vulnerabilities and implement risk mitigations. The Saudi model included a combination of assessments (such as penetration testing, vulnerability assessment, compromise assessment, and cybersecurity architecture and configuration review). Given the high number of assessments required to ensure the security of an event on the scale of the G20, the Saudi model combined direct assessments conducted by G20 Secretariat with entities' self-assessments. A mitigation plan should be developed to reduce the risk of cyber attacks and should involve the creation of a dedicated incident response team aside from the regular team.

Audience Understanding and Engagement – Mega events like the G20 include a variety of internal and external stakeholders, and awareness campaigns are crucial to educating participants on the importance of cybersecurity. It is essential to identify the appropriate audience for these sessions and to involve relevant individuals with specific G20 roles and duties. Campaigns and training exercises should be tailored to each group's responsibilities to achieve effective outcomes. By providing visibility on the implications of certain decisions in case of an attack and establishing clear communication channels, participants can be encouraged to develop an agile and collaborative mindset, and the overall cybersecurity readiness and resilience of the Program is promoted.

Key Statistics for the G20 Cybersecurity Readiness and Resilience Program

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

385K+
Cyber attacks detected

361
Cyber threats analyzed and handled

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

Introduction

This report offers guidance on cybersecurity best practices for countries hosting future G20 Presidencies and similar mega events.

In 2020, the Kingdom of Saudi Arabia held the rotating Presidency of the G20. The Presidency is an opportunity to influence the agenda of a complex and rapidly changing global environment.

The increasingly networked nature of the global economy elevates the importance of economic systems' digital security, which encompasses the value of global collaboration. Therefore, during Saudi Arabia's presidency year, the G20 Digital Economy Task Force(DETF) introduced a priority titled Security in the Digital Economy, which was aligned with the Presidency year's overall theme and goals.

Throughout 2020, the DETF worked on the outcome of the Security in the Digital Economy priority along with multi-stakeholders including the Business 20 (B20) Engagement Group and related international organizations. The outcomes of these efforts were captured in:

- July 2020, with the release of the 2020 Digital Economy Task Force Ministerial Declaration and the G20's Annex related to Security in the Digital Economy, and

- November 2020, when the priority and its outcome were endorsed by the G20 leaders in the G20 Riyadh Summit Leaders Declaration.

In addition, the DETF hosted the G20's first event entirely dedicated to cybersecurity: the G20 Cybersecurity Dialogue.

The G20 Cybersecurity Readiness and Resilience Program, led by the NCA, was originally designed for an in-person G20 Presidency. However, as the COVID-19 pandemic evolved throughout 2020, it became clear that an in-person event was going to be difficult. For this reason, an executive decision was made to move the entirety of the Presidency, including the Leaders' Summit, to a digital format. This required the Program's team to mobilize with an expanded focus on cybersecurity.

Compared to other mega events that last a few days, weeks, or at most a couple of months, the G20 lasts one year. It includes numerous meetings featuring ministers, senior government officials, and civil society representatives. In addition to being a key topic of discussion during the G20, cybersecurity was also a crucial consideration in the planning, organization, and execution of the events themselves, especially since the majority of the events were held virtually for the first time in the history of the G20 Presidency.

This report examines how cybersecurity was integrated to secure the G20 Presidency year. It captures, analyzes, and documents cybersecurity activities and discussions prior to the beginning of the G20 Presidency until the end of the Leaders' Virtual Summit.

By presenting the Saudi model for strengthening cyber resilience during the G20 Presidency year, this report highlights the importance of international collaboration to improve global cybersecurity resilience. It presents the model that the Kingdom developed for securing the 2020 G20, which mirrors the joint efforts between NCA, its operational arm, the Saudi Information Technology Company(SITE), and other key service providers. Also, the report identifies lessons learned. Ultimately, this is a guideline on cybersecurity best practices for countries hosting future G20 Presidencies, or similar mega events.

G20 Cybersecurity Readiness and Resilience Program

The G20 Cybersecurity Readiness and Resilience Program was launched to augment the cyber resilience of the G20 Saudi Secretariat and related entities.

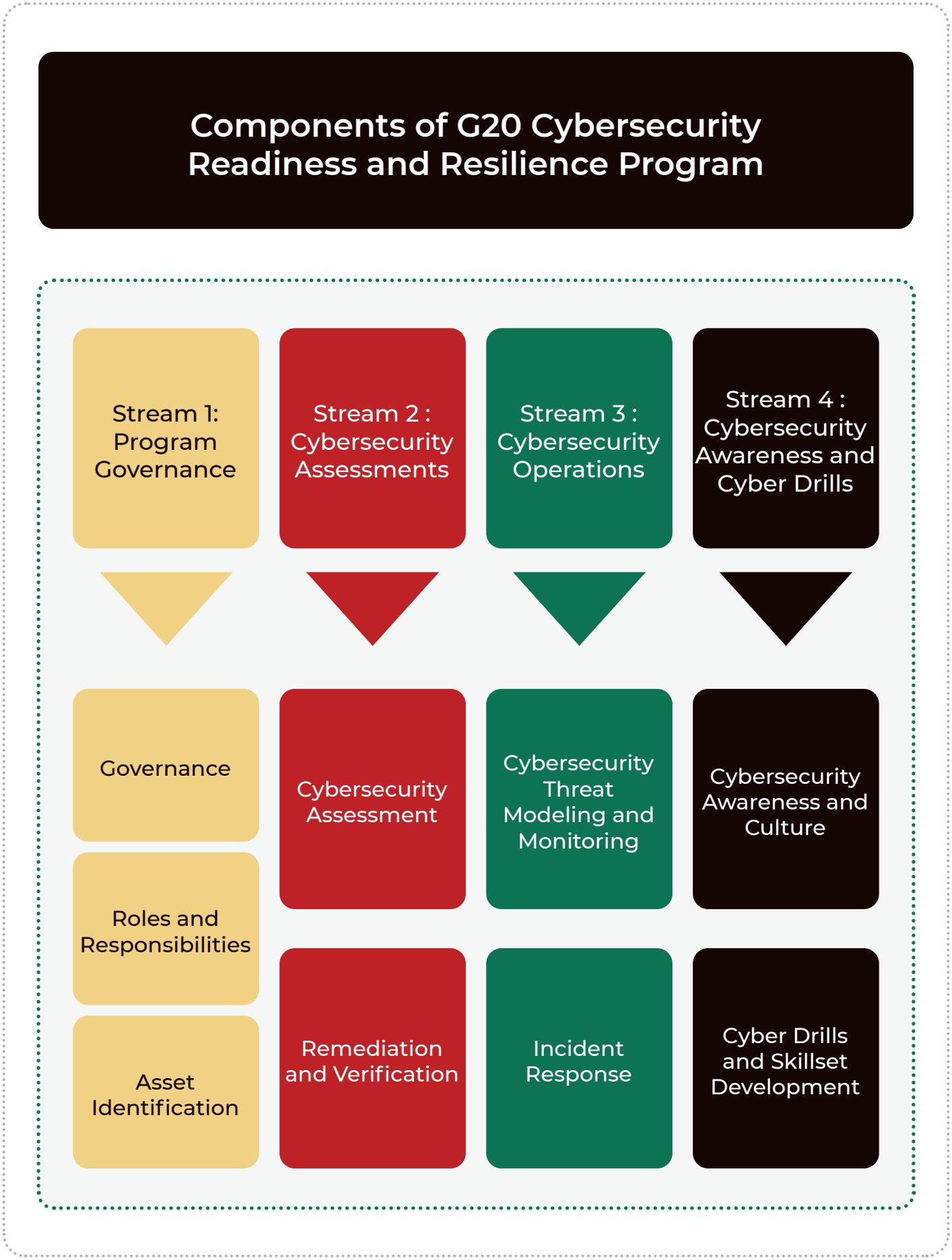

Components of G20 Cybersecurity Readiness and Resilience Program
Stream 1: Program Governance
Stream 2 : Cybersecurity Assessments
Stream 3 : Cybersecurity Operations
Stream 4 : Cybersecurity Awareness and Cyber Drills
Governance
Roles and Responsibilities
Asset Identification
Cybersecurity Assessment
Remediation and Verification
Cybersecurity Threat Modeling and Monitoring
Incident Response
Cybersecurity Awareness and Culture
Cyber Drills and Skillset Development

Figure 2.

The G20 Cybersecurity Readiness and Resilience Program was launched to augment the cyber resilience of the G20 Saudi Secretariat and all related entities, including third parties.

The G20 Cybersecurity Readiness and Resilience Program followed a model based on three principles:

1

Firstly, **inclusiveness**, which entailed identifying key stakeholders involved in receiving, hosting, transporting and protecting the participants. This included the creation of a Cybersecurity Function within the G20 Saudi Secretariat.

2

Secondly, the principle of **resilience** was informed by an understanding of the complexity of cyberspace and the cybersecurity challenges of securing a G20 Presidency. This understanding enabled the creation of a model based on resilient and verified defenses that were capable of withstanding and responding to cyber threats, while simultaneously detecting and remediating vulnerabilities at an early stage. Awareness campaigns were conducted across all stakeholders to foster a culture of cybersecurity throughout the G20 Presidency and the Leaders' Summit.

3

Thirdly, **collaboration**, which involved connecting a complex ecosystem comprised of public and private entities nationally and internationally. The resulting partnerships fostered trust and confidence across all entities and enabled the model to achieve high levels of participation. Ultimately, the joint efforts between NCA, its operational arm, the Saudi Information Technology Company(SITE), and other key service providers, led to the success of the model.

The Approach

The approach followed focused on leveraging international experiences and the NCA's expertise to develop a customized model. To this end, an initial benchmark exercise was conducted to build on previous experiences as depicted in Figure 3 below:

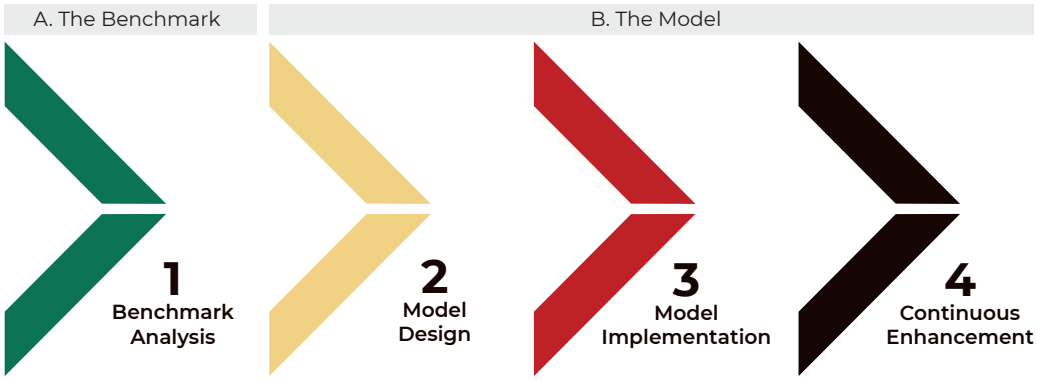


Figure 3.

A. The Benchmark

The complexity of planning, organizing, and executing mega events, such as a yearlong G20, requires a deep understanding of previous experiences. One of the main challenges discovered from the outset of 2020 G20 planning was the lack of publicly available data from previous events. Furthermore, in many instances, the teams responsible for securing the G20 Presidencies are only created and maintained for the duration of the event. Once the G20 Presidency has concluded, the individuals on these teams return to their previous roles.

This results in the loss of valuable institutional knowledge and makes the identification of data extremely challenging. For this reason, the creation of a cybersecurity-focused Saudi model was informed by a benchmark and gap analysis of other mega events beyond the G20.

Mega events have always been attractive targets for cyber attacks, which have become more prevalent due to growing dependence on digital channels and new technologies. The benchmark included the identification and analysis of common cyber adversaries, threats, and attack patterns.

The growing digitalization of these events can be seen in the increase in broadcasting, in interactions before and during the events, and through digital communication channels and conferencing.

Cyber threat actors can now use many tools to gain unauthorized access to critical information that could inflict significant damage when exploited.

Cyber Threat Actors

Cyber threat actors can vary depending on their motives and targets. In the context of mega events, they include:

Nation-states

Terrorists/ Criminal organizations

Hacktivists

Competitors

Insider Threats

Such threat actors commonly target systems, devices, and the infrastructure of the main stakeholders, whether these are event participants, organizers, or the general public.

Common Cyber Threats

Recent G20 and mega events (analyzed as part of the benchmark) demonstrate that, while cyber events during these major summits can total in the hundreds of thousands, only a small fraction of these incidents were reported. Analysis shows that main threats during such events are:

Data breaches – A threat in which unauthorized access and data exfiltration occur. Adversaries could send phishing invitations to the events' participants. Such invitations could have a link with malware to enable access to sensitive information and, consequently, lead to the loss of personal and financial information, as well as other classified documents.

Denial of service – A distributed denial of service (DDoS) attack could impair the official event website, and participants could be unable to access the events' information. Attacks like this can start even before the opening ceremony and target third parties responsible for the events' online services. DDoS temporary disruptions could open up an opportunity for cyber attackers to access the online platform and steal data.

Personal account compromise – A threat in which personal account information - for example, a username and password - is compromised by an adversary who can subsequently steal private information or demand a payment for retrieval of the stolen account.

Personal device compromise – A threat in which adversaries take control of a device and perform illegal actions, including but not limited to stealing valuable data.

Compromise of surveillance camera & security equipment – A threat in which adversaries penetrate surveillance and security equipment, resulting in inhibited security or loss of control.

Attacks on event infrastructure – Cyber attacks can impact an event's infrastructure by infiltrating it through social engineering, malware, and other attack vectors. This can have a significant impact on the event and may lead to physical harm.

Insider threat – A threat to an organization that comes from actors within the organization, such as employees, former employees, contractors, or business associates.

Key Takeaways

When benchmarking mega events, their cybersecurity setups were analyzed and five key takeaways emerged:

Organization of the event's cybersecurity – Recent events have relied on outsourcing cybersecurity to dedicated firms.

Types of cyber threats – The most common cyber threats impacting mega events are fictitious emails containing malicious attachments and links.

Targets of cyber threats – Government officials and delegations, as well as organizers and third party service providers, are the main targets.

Volume of cyber attacks – When analyzing all the events, it appears that the volume of cyber attacks increases each year, demonstrating the impact of digitalizing mega events.

Timing of cyber attacks – Cyber attacks were mainly observed in the days leading up to the summit, as well as during opening ceremonies.

Best Practices

Accordingly, analysis of previous experiences and the NCA's own expertise allowed further identification of six best practices for securing mega events, including a G20 yearlong Presidency:

1. **Strategic planning and horizon scanning**: At the beginning of any cybersecurity planning, the strategic objectives should be defined and threat analysis appropriately conducted.

2. **Governance**: A clear governance model, enabled by a well-resourced team and an oversight steering committee whose members include the cybersecurity management team, cybersecurity situational awareness capabilities, incident response team, and other relevant governmental and private sector stakeholders. The steering committee enables effective decision-making and coordination.

3. **Asset management**: Critical systems and networks, including those of third-party providers and external entities, are identified and enhanced to increase cybersecurity readiness.

4. Dedicated monitoring, assessment, and response team: Continuous cybersecurity assessment, monitoring, hunt and response teams are established to collect and analyze data from government agencies and third-party providers and to respond to cyber attacks/incidents.

5. Information sharing: Information sharing between engaged stakeholders is encouraged and often enabled through dedicated information sharing platforms.

6. Cybersecurity awareness and cyber drills: Cybersecurity awareness training programs are carried out for employees and key stakeholders, including third party providers, to ensure they follow cybersecurity guidelines.

B. The Model

In light of the analysis of previous mega events, it is evident that cybersecurity cannot be limited to certain areas. Rather, it represents a core activity in the preparation and conduction of a successful G20 Presidency. For this reason, Saudi Arabia developed a model to ensure cyber resilience and secure the entire G20 Presidency. The design of the Saudi model, applied throughout the Presidency year, followed a two-tier approach:

Tier 1

It consisted of strengthening the cybersecurity readiness and resilience of the G20 Presidency year and was enabled by the comprehensive governance model, which focused on two main areas: the G20 Saudi Secretariat's Cybersecurity Function and coordination with all related stakeholders.
The G20 Saudi Secretariat's Cybersecurity Function covered:

- **Supporting and facilitating the execution of the Program.**
- **Identifying information technology assets.**
- **Monitoring all assets closely.**
- **Establishing a dedicated incident response team for the G20 Saudi Secretariat.**
- **Conducting cybersecurity assessments.**
- **Analyzing and remediating cybersecurity vulnerabilities.**

The related stakeholders' focus areas covered:

- **Complying with NCA requirements.**
- **Conducting cybersecurity self-assessments.**
- **Analyzing and actioning all findings related to cybersecurity assessments.**
- **Reporting cybersecurity incidents.**

Tier 2

It represented the activation of the cybersecurity model with the Leaders' Virtual Summit as a focused dimension. The Leaders' Virtual Summit was held virtually for the first time in history and was treated as a smaller version that mirrored the model applied throughout the G20 Presidency year. However, the model was scaled up to elevate the relevant capabilities in accordance with the depth and complexity required to prepare for and secure this specific event. Roles and responsibilities were also tailored to the specific requirements of the Leaders' Summit. All information technology and platform assets were closely monitored, and a mitigation plan was specifically enforced to reduce the risk of cyber attacks; thus a dedicated incident response team was established to complement the efforts of the regular team. Finally, several specific cyber drills tailored to the Leaders' Virtual Summit were conducted to prepare and synergize responses to potential cyber attacks.

Summary of the Saudi Cybersecurity Model

While the model had always been envisioned to integrate cybersecurity, further enhancements were conducted in the design phase to accommodate the moving of the G20 from an in-person to a wholly digital series of events, including the Leaders' Summit. The final model was designed accordingly:

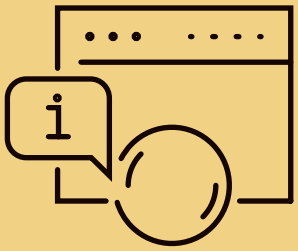
Streams	Tier 1 – Strengthening Cyber Resilience During the Presidency Year	Tier 2 – Strengthening Cyber Resilience During the Leaders' Virtual Summit
Program Governance	• Established an executive committee & technical team and Identified a set of stakeholders: – G20 Saudi Secretariat – Executive Committee – NCA – Service providers – Third parties – Related entities – Saudi Information Technology Company (SITE) • Information Technology Assets Identification and Protection • Developed specific cybersecurity requirements	• Detailed roles & responsibilities • Enhanced involvement of key stakeholders: – G20 Saudi Secretariat – Executive Committee – NCA – Service providers – Third parties – Related entities – Saudi Information Technology Company (SITE) • Daily coordination at senior leadership level • Accelerated decision-making
Cybersecurity Assessments	• Conducted a set of cybersecurity assessments with emphasis on the G20 Saudi Secretariat and the digital infrastructure and platform providers: – Risk Assessment – Penetration Testing – Vulnerability Assessment – Compromise Assessment – Compliance Assessment – User Access Review – Cybersecurity Architecture and Configuration Review	• Conducted a set of cybersecurity assessments with emphasis on the G20 Saudi Secretariat and the digital infrastructure and platform providers: – Risk Assessment – Penetration Testing – Vulnerability Assessment – Compromise Assessment – Compliance Assessment – User Access Review – Cybersecurity Architecture and Configuration Review

Cybersecurity Operations	• Threat modeling • incident response • Cybersecurity monitoring and situational awareness	• Microfocus on the National Digital Infrastructure Service Provider • Augmented cybersecurity protection measures • Threat modeling • Elevating the incident response capabilities and dedicating a national IR team for the Virtual Summit • Close cybersecurity monitoring on the G20 Saudi Secretariat and the digital infrastructure and platform provider
Cybersecurity Awareness and Cyber Drills	• Cyber drills tailored toward the whole Presidency year • Workshops tailored to all stakeholders • Awareness campaigns	• Cyber drills tailored toward the Leaders' Virtual Summit • Workshops tailored toward the engaged stakeholders • Awareness campaigns

Tier 1 - Strengthening Cyber Resilience During the Presidency Year

Stream 1: Program Governance

A key step in mobilizing a large program and its components is developing a foundation to ensure its success. As a foundation-building exercise, program governance includes the creation and establishment of an organizational structure, where the program's scope is identified, clear roles and responsibilities are awarded to different stakeholders, and the relationship between different functions is identified. Oversight mechanisms are implemented to ensure continuous review and guarantee that the necessary adjustments are made. This entire process is crucial to achieving the intended outcome of securing the G20 Presidency.



The preparation and the execution of the Program lasted for more than **400 days**.

A. Program Governance

The Program's governance ensured effective coverage of all the various G20 aspects. The overall governance structure is represented in Figure 4, and it was built on two main principles: Unification, and collaboration. Ultimately, the joint efforts between NCA, its operational arm, the Saudi Information Technology Company(SITE), and other key service providers, enabaled the model to succeed.

B. Roles & Responsibilities

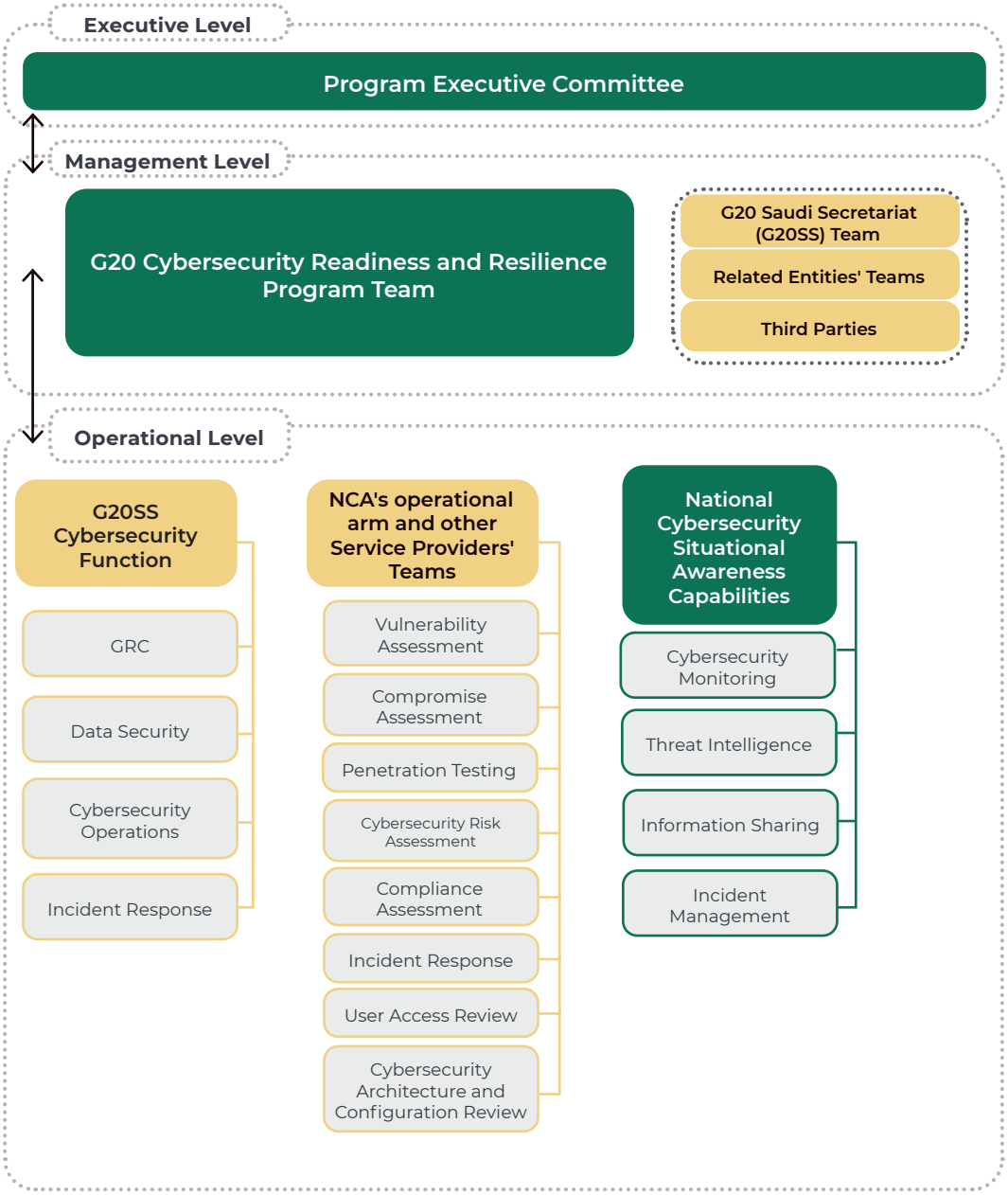


Figure 4.

Building upon the strategic governance structure, the subsequent phase was based on the identification of key stakeholders, who were categorized into three levels of oversight: executive, management, and operational engagement. Overall, more than 100 entities and 400 cybersecurity specialists participated in the program. Each stakeholder's roles and responsibilities were codified based on their relevance to the G20 Presidency, accordingly:

Executive Level

Program Executive Committee: Led by

the NCA, it consisted of other members, including the G20 Saudi Secretariat and key service providers such as NCA's operational arm, the Saudi Information Technology Company (SITE), the Telecom and Technology Providers, the Cybersecurity Solutions and Services Providers, and the National Digital Infrastructure Service Provider, which hosted the national Digital Infrastructure of the Leaders' Summit virtual platform in Tier 2. The role of the Committee was to oversee the evolution of the Program by periodically producing and circulating reports and cyber indicators aiming to assess the risks that the Presidency faced. It was ultimately responsible for overseeing remediation plans and for the escalation and communication of any activity. The Executive Committee held meetings on a regular basis, and more than 450 reports were released.

Management Level

G20 Saudi Secretariat (G20SS) Team: The primary stakeholder, responsible for coordination and participation in all activities related to the Kingdom G20 Presidency and application of the cybersecurity requirements. For the first time in the history of the G20, the Saudi Secretariat built a Cybersecurity Function that was specifically tasked to support cybersecurity internally, within the Secretariat only.

G20 Cybersecurity Readiness and Resilience Program Team: The NCA led the overall Program management and supervised its implementation in collaboration with the G20 Saudi Secretariat and other Service Providers, including NCA's operational arm, the Saudi Information Technology Company (SITE), the Telecom and Technology Providers, and the Cybersecurity Solutions and Services Providers. In addition, it was responsible for the establishment of cybersecurity requirements to ensure the cybersecurity resilience of both the G20 Presidency in Tier 1 and the Leaders' Virtual Summit in Tier 2. In preparation for the Leaders' Virtual Summit, the National Digital Infrastructure Service Provider also joined the Program Team as host of the Leaders' Virtual Summit to address the activities of Tier 2.

Related Entities' Teams: These consisted of directly involved national entities that participated in regular workshops and meetings.

Third Parties: This included any external third party related to the G20 Presidency, across a wide range of entities. This also included airports and hotel service providers responsible for hosting guests when the G20 was to be held physically.

Operational Level

Cybersecurity Function within the G20 Saudi Secretariat: Responsible for incorporating governance, risk management, and compliance capabilities with elements of data security and incident response in the broader cybersecurity operations that were conducted in preparation for and throughout the Presidency year. Additionally, managed cybersecurity services were provided to the cybersecurity function within the G20 Saudi Secretariat by NCA's operational arm, the Saudi Information Technology Company (SITE).

National Cybersecurity Situational Awareness Capabilities: The team, led by the NCA and comprised of cybersecurity service providers, such

as NCA's operational arm, the Saudi Information Technology Company (SITE), was responsible for 24/7 cybersecurity monitoring and situational awareness, analyzing cyber threats and risks, sharing information (detailed reports of possible threats) with related entities and the G20 Saudi Secretariat, and providing support for incident management.

NCA's Operational arm and other Service Providers' Teams: Service providers were grouped into two categories: digital infrastructure hosts and cybersecurity service providers. For Tier 2, the National Digital Infrastructure Service Provider hosted the platform for the Summit with the Telecom and Technology Provider. The key cybersecurity service providers, including NCA's operational arm, the Saudi Information Technology Company (SITE), supported the G20 Cybersecurity Readiness and Resilience Program by providing cybersecurity services. Service providers were also responsible for conducting vulnerability scanning, compromise assessments, penetration testing, cybersecurity risk assessments, and compliance assessments. In addition to that, tight collaboration was in place to provide timely incident response support.

C. Asset Identification

An exercise leading up to the Presidency was con- ducted to identify and classify all information technology assets related to the Presidency into an inventory, whether they were directly or indirectly connected to the G20 Saudi Secretariat.

Stream 2: Cybersecurity Assessments

A series of practical and effective assessments were carried out to evaluate the information technology assets from a cybersecurity perspective, these assessments were conducted by NCA's operational arm, the Saudi Information Technology Company(SITE), and other key service providers, and it included the following assessment activities:

Risk Assessment: A mechanism to identify cyber risks of an information technology asset, whether hardware or software, by determining the probability of occurrence and the impact of a cyber attack.

Penetration Testing: A simulation of a cyber attack targeting digital infrastructure. Its usefulness de- rives from helping administrators and stakeholders discover key exploitation points and test procedures in case of a breach. Penetration testing can also uncover vulnerabilities in security processes and therefore help prevent the damaging effects of attacks.

Vulnerability Assessment: A vulnerability assessment is conducted on all information technology assets to determine any known cybersecurity vulnerability.

Compromise Assessment: A valuable technique to identify and analyze any sign of an ongoing breach.

Compliance Assessment: An assessment that enables identifying any gap between the existing controls in place and what is mandated by the national cybersecurity

authority (NCA 's Essential Cybersecurity Controls). By determining any potential risk of non-compliance, it supports all entities to understand their compliance risk exposure.

User Access Review: An assessment that enables organizations to periodically evaluate and verify that only legitimate users maintain access to the infrastructure, thus minimizing the risk of unauthorized access.

Cybersecurity Architecture and Configuration Review: An assessment that helps to identify cybersecurity weaknesses in the architecture, and cybersecurity configurations' inconsistencies and vulnerabilities of different infrastructure components.

More than **120 cybersecurity assessments** were routinely conducted throughout the year-long Presidency to identify vulnerabilities and risks among related entities. Over **100 entities** were assessed.

Assessment Lifecycle

The assessments were conducted on information technology assets in place on a two-phased methodological approach. While a direct assessment was conducted on the G20 Secretariat and any other directly related entities, a number of self-assessments were also requested to be conducted by the other entities in scope.

All threats and vulnerabilities reported were organized within a prioritization scheme that defined priorities over the particular attack's impact.

As part of the methodological approach to identify and remediate vulnerabilities, a number of recommendations emerged from the evaluation; these were escalated through various stakeholders and addressed on a phased approach, prioritizing urgent requirements.

Ultimately, verification of all the activities in scope for the remediation plans was undertaken and applied to ensure proper resolution.

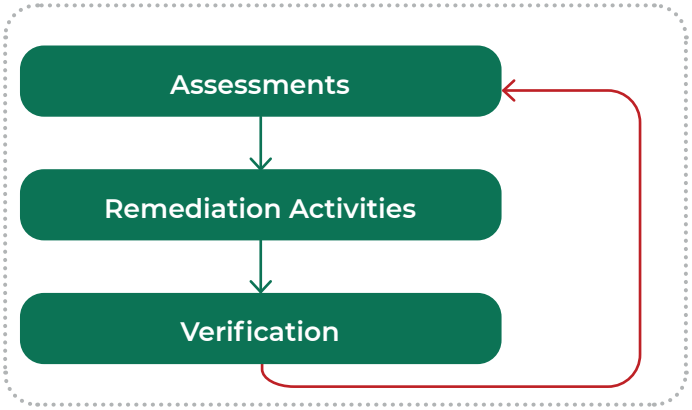


Figure 5.

Stream 3: Cybersecurity Operations

In parallel to the routine conduction of cybersecurity assessments, a number of cybersecurity operations were performed throughout the Program's lifecycle.

Threat Modeling, Cybersecurity Monitoring, & Incident Response

Due to the increasing digitalization of operations and the expanding attack surface, the volume of cybersecurity threats is growing exponentially. The primary purpose and objective of this phase was therefore to enhance cybersecurity readiness and resilience vis-à-vis an attack, in order to protect the cyber space around the G20. Cybersecurity capabilities were developed by enacting cybersecurity protection services and solutions, including DDoS mitigation and email protection. This phase consisted of identifying a mechanism to control and respond to threats. Three stages were envisioned as part of the process: threat modeling, cybersecurity monitoring, and incident response and management.

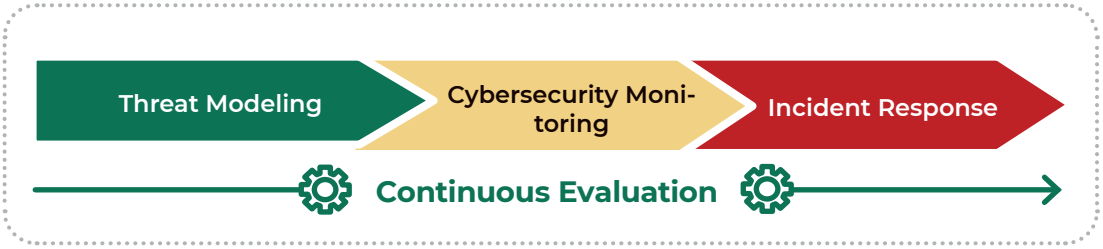


Figure 6.

Based on best practices, a comprehensive set of **Threat modeling** techniques were adopted to classify, examine, and model cybersecurity threats related to the assets in scope. Threat modeling is a process that allows for a structured approach to identify and address cyber threats by rating them according to severity and probability of occurrence.

By allowing the team to identify cyber attackers' tactics, techniques, and procedures (TTPs) faced during the G20 Presidency year, the cybersecurity team was prepared to respond to attacks resulting from these threats, enhancing cyber readiness and resilience.

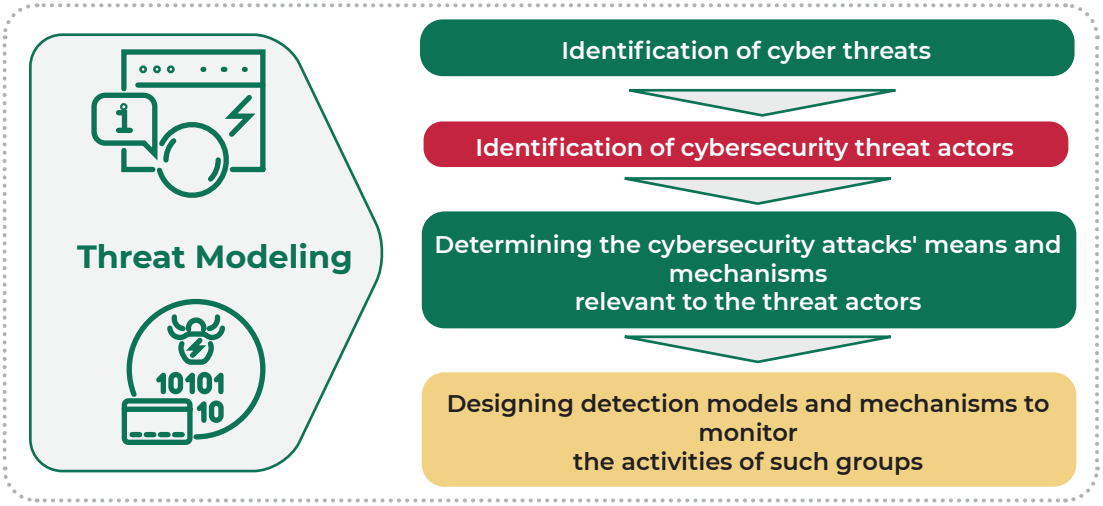


Figure 7.

A matrix was designed to assess the threats, considering the importance of the information technology asset and the threat level. These resulted in four categories: critical threats, high threats, medium threats, and low threats.

24-hour **cybersecurity monitoring** was implemented to oversee the various information technology assets relevant to the G20 Saudi Secretariat, as well as the Program's infrastructure and assets.

A total of more than **10,000 hours** of continuous cybersecurity monitoring was conducted.

This helped provide visibility on potential cybersecurity threats that could hinder full and continuous defense capabilities. Three levels were identified as requiring monitoring to develop situational awareness: firstly, cybersecurity as a whole at the national level and as a core business responsibility; secondly, the key stakeholders of the G20 Presidency; and, finally, the G20 Secretariat.

As a result, more than **600 cybersecurity alerts** were shared with the relevant entities. The vulnerabilities and threats highlighted in the cybersecurity alerts were remediated and closed at a fast pace.

The **incident response** stage was the final feature of this third phase, developed to ensure prompt readiness in the management of and response to cybersecurity incidents throughout the Presidency period. To this end, incident response teams were created, which consisted of teams from NCA's operational arm, the Saudi Information Technology Company, and other key service providers, to respond to incidents on three levels: at the national level, the G20 Saudi Secretariat level, and specifically, the level of the Leaders' Summit.

Stream 4: Cybersecurity Awareness and Cyber Drills

The final phase focused on building cybersecurity awareness and conducting cyber drills. These elements are crucial to an engagement strategy that is able to identify where the cybersecurity knowledge gaps are and what specific components of the model require tailored thinking. Building awareness through different activities promotes a strong and constructive attitude among key stakeholders, who learn to quickly adapt. As such, it is a powerful way to secure the events, the people, and the assets, while ensuring cybersecurity readiness and resilience. These were all enabled by the existing National Cybersecurity Academy Program.

A. Cybersecurity Awareness

This phase of the model was centered on raising cybersecurity awareness. This relates to the crucial importance of the human factor – a key component of a cyber-resilient infrastructure – in implementing and achieving a cyber-secure ecosystem. Social engineering can be carried out by exploiting human psychological vulnerabilities. While technology solutions can be implemented to improve infrastructure security, "insider threats" – an insider harming an organization by leveraging their privileged level of knowledge and/or access – can still occur.

A series of general cybersecurity awareness programs was developed for the participating stakeholders – capitalizing on the Saudi CERT's content – to increase **awareness**. These programs aimed to educate the audience on information protection, acceptable use of technology, and incident identification and response. Quarterly cybersecurity awareness sessions were conducted.

B. Cyber Drills

Workshops were organized for the Program's members from relevant organizations, to clarify roles, responsibilities, and requirements related to the cybersecurity of the Program and to enable continuous coordination. During these workshops, key stakeholders exchanged threat intelligence and best practices for responding to emerging cybersecurity threats.

Further **training** was routinely provided to key staff members to equip them with high-quality technical and non-technical cybersecurity knowledge.
As part of the G20 Cybersecurity Readiness and Resilience Program, several **cyber exercises**, including cyber drills, were carried out in preparation for the Presidency.

Cyber drills are simulations of potential cyber attacks and incidents. They provide a way to test the effectiveness of the incident detection and response strategy, promote cooperation to raise the level of readiness and coordination between involved entities, and enhance cybersecurity capacity and awareness to respond to various cyber risks and threats. They are important not only from a cybersecurity perspective, but also to ensure that all stakeholders are aware of preparation, remediation, and mitigation efforts.

Several exercises were conducted – mainly aimed at national entities relevant to the G20 and other significant stakeholders – as interactive sessions to immerse cyber incident responders in multiple simulated cyber scenarios. The scenarios included four types of attacks: data breaches, malicious software, website defacement, and DDoS attacks.

The methodology considered the key stages of cyber incident response. These stages help to assess the comprehension of processes and implications of decisions and actions during simulated incidents.

The results of the cyber drills were analyzed to identify and categorize the main strengths and development areas of each entity in scope. These informed the mitigation actions that were executed to overcome any shortage and ensure timely and appropriate response capabilities to enhance the cybersecurity of the Presidency year and, in particular, the Leaders' Virtual Summit.

More than **9 cyber drills** were conducted, engaging more than **100 entities**.

More than **60 workshops** were conducted for related entities with the participation of the relevant Chief Information Security Officers.

Tier 2: Strengthening Cyber Resilience During the Leaders' Virtual Summit

The G20 Leaders' Summit brings together heads of state or government from 19 countries and the European Union, as well as leaders of guest countries and representatives of invited regional and international organizations. The 2020 G20 Leaders' Summit was held virtually on November 21 – 22 and chaired by The Custodian of the Two Holy Mosques, King Salman bin Abdulaziz Al Saud. The G20 Presidency built on the success of the extraordinary virtual G20 Leaders' Summit held in March and the outcomes of over 100 virtual working groups and ministerial meetings. As such, it was the most important event of the G20.

The importance of the Leaders' Virtual Summit required it to be treated as a smaller version that mirrored and strengthened the approach taken to secure the G20 Presidency year. This was particularly crucial as the Leaders' Virtual Summit was held over multiple locations, adding to the complexity of the operation, as additional resources were needed to ensure appropriate cybersecurity readiness.

For Tier 2, each stage of the designed model was replicated and enhanced to secure the Virtual Summit, accordingly:

Program Governance

The roles and responsibilities present in the executive, management, and operational level of Tier 1 were tailored to a smaller number of key stakeholders, now including daily coordination with the National Digital Infrastructure Service Provider, responsible for hosting the Virtual Summit.

Cybersecurity Assessments

A variety of cybersecurity assessments, with emphasis on the National Digital Infrastructure Service Provider, were undertaken, including penetration testing, risk assessments, vulnerability assessments, compromise assessments, compliance assessments, user access reviews, and cybersecurity architecture and configuration reviews.

Cybersecurity Operations

The National Digital Infrastructure Service Provider hosting the Virtual Summit and the G20 Saudi Secretariat were closely monitored and a mitigation plan was specifically enforced to reduce the risk of cyber attacks. This included cybersecurity protection services and solutions such as DDoS mitigation and email protection.

To further mitigate any risk of potential gaps in the Program arising from external, unforeseeable factors that could hinder the Leaders' Summit, an additional incident response team was established in addition to the regular incident response team. This additional team was composed of available incident response professionals in Saudi Arabia, who were identified so their expertise could be pooled to ensure they would be ready to act as back-ups in the event of an incident.

Cybersecurity Awareness and Cyber Drills

In addition to regular cyber drills, a number of specific drills, tailored toward

the Leaders' Summit, were conducted to prepare and synergize responses to any potential cyber attack. Awareness campaigns and workshops were enhanced to support the preparation and ensure the summit was conducted smoothly, with all stakeholders involved trained and prepared to face any potential adverse event.

The cybersecurity plan implemented specifically for the Virtual Summit was a key element of the G20 Cybersecurity Readiness and Resilience Program. It was developed to protect key critical assets while also allowing the event to run smoothly. In and of itself, it represents a strategy to efficiently secure a global event, as well as an achievement in the realization of cybersecurity readiness and resilience.

Figure 8.

Recommendations and Lessons Learned

A number of lessons learned and recommendations have emerged from the experience of the Kingdom's G20 Presidency.

Leadership Engagement and Support

As the world was rapidly slipping into the pandemic, leadership engagement proved crucial in promptly realizing what was happening and in providing a new strategic vision to strive towards.

The executive decision made to move the entirety of the G20 Presidency to digital platforms opened up a new paradigm for hosting and securing mega events. This change was only possible as the leadership involved built on the foundation of the original model and enhanced the Program's governance and activities. As the effects of the pandemic revealed themselves and the threat landscape evolved accordingly, oversight mechanisms and consistent support by the leadership were implemented to ensure continuous review and prompt adjustments.

Ultimately, national leadership empowered the G20 Saudi Secretariat by mobilizing resources and capabilities to ensure the success of the model and the fulfillment of the G20 Cybersecurity Readiness and Resilience Program to secure the G20 Presidency and the Leaders' Summit.

Value of Data, Governance, and Model Design

Finding sufficient data and relevant information on previous G20 experiences and other mega events is a complex exercise. While there is no recognized methodology or approach that can be drawn from the international stage, designing a model is of paramount importance to the establishment of a successful and long-standing strategy. It is of vital importance to develop and document the experience to contribute to the wider cybersecurity community.

It is therefore strongly recommended to conduct workshops in collaboration with previous mega event hosts, where data and information can be shared and analyzed. The main takeaways extrapolated from the data collected are pivotal to the identification of areas and dimensions that are relevant to the event itself. In turn, these areas need to be analyzed against a model that allows the extrapolation of the purpose, objective, and aims, which subsequently clarify the identification of the talent and expertise required. In addition to this, creating a team of national stakeholders - including third parties - and defining their roles and responsibilities in each area helps to create synergies across various areas of expertise. Ultimately, codifying roles and responsibilities enables the model to be resilient in the face of adverse events, as each stakeholder is fully aware of their function and responsibilities in tackling any impediment and enhancing the model.

The Saudi model offers a recommended approach for future G20 Presidencies. Its focus on creating a Cybersecurity Function within the G20 Secretariat ensures that cybersecurity had a key role and representation on both management and operational levels.

Need for Agility and Coordination with Partners

The COVID-19 pandemic has touched every corner and aspect of the world, inflicting long-term implications on our lives. As the pandemic unfolded throughout the Presidency, it became clear that holding events in person was going to be a risk to citizens across the Kingdom and across the globe. As nations began to shield themselves in an attempt to fight the spread of the

virus, an executive decision was made to move the entirety of the Presidency, including the Leaders' Summit, to the digital realm. The value of digitalization and secure connectivity became clear as a viable and practical alternative to holding physical events.

Securing a wholly digital G20 was achieved because the model in place was based on flexibility, agility, and a commitment to bounce back from any adverse events. While the original model included cybersecurity at its core – and thus ensured cybersecurity readiness and resilience – a number of additional and urgent activities needed to be promptly implemented.

With the increase of attack vectors and the potential impact of cybersecurity attacks, the model was swiftly enhanced to involve new stakeholders and use strong partnerships to increase capacity and elevate existing cybersecurity monitoring. The roles and responsibilities of key stakeholders were repurposed to develop even stronger communication and coordination, and remediation and escalation points were created to ensure prompt responsiveness and improve cybersecurity resilience.

Early Preparation and Scalable Efforts

The G20 consists of a series of meetings, events, and workshops. Holding them virtually meant adapting and scaling up efforts to secure them. Early preparations for the G20 are a key step in the process, as they reveal gaps where more expertise and capabilities are needed while still allowing time for these needs to be addressed.

The NCA Incident Management process was tailored to accommodate the G20. This allowed the Presidency to ensure stakeholders followed a consistent approach to cybersecurity incident management.

It is recommended that dedicated incident response teams are formed not only for the G20 as a whole, but also for events of crucial importance, such as the Leaders' Summit. Scaling up incident response capabilities makes it possible for specialists to respond to multiple incidents simultaneously.

It is also recommended best practice to build on existing plans, capabilities, and methodologies across domains, as these often only need to be adapted, tailored, and enhanced to fit specific circumstances.

Scope Management

Identifying direct and indirect critical assets is a primary step to secure a mega event. These include both information technology and event assets, whose ownership should be assigned to ensure that each stakeholder is clear on their roles and responsibilities.

External dependencies, third parties, and supply chains should be identified and taken into consideration to allow adequate mitigation plans. There should be a balance between allowing these entities to operate independently and providing the adequate level of cybersecurity protection and monitoring. A homogeneous approach, regardless of diverse geographical distribution, should be established and tightly coordinated. It should be enabled by the development of strong and effective partnerships, as well as active information sharing, with all the key stakeholders.

Ultimately, when managing the scope of the Program, infrastructure protection of all related entities in the larger G20

ecosystem should be accounted for, given the variance in cybersecurity capabilities and skills that often exists between entities.

Importance of Regular Cybersecurity Assessments

Through regular assessments, the professionals responsible for G20 cybersecurity can promptly identify assets' vulnerabilities and implement risk mitigations. The Saudi model included a combination of assessments, such as penetration testing and vulnerability assessment, compromise assessment, and cybersecurity architecture and configuration review. Given the high number of assessments required to ensure the security of an event on the scale of the G20, the Saudi model combined direct assessments conducted by the G20 Secretariat with entities' self-assessments. A mitigation plan should be developed to reduce the risk of cyber attacks and should involve the creation of a dedicated incident response team aside from the regular team.

Audience Understanding and Engagement

Mega events like the G20 include a variety of internal and external stakeholders. Awareness campaigns are crucial to highlight the importance of cybersecurity and enable individuals to contribute to cybersecurity, rather than increase risk.

To ensure this process achieves its desired outcomes, it is important to identify the appropriate audience for these campaigns, including individuals who may have specific roles and responsibilities. Awareness campaigns should be tailored accordingly, based on the stakeholders' knowledge of cybersecurity.

Cyber drills, workshops, and training demonstrate to participants the cyber threats and risks faced by the event, along with their responsibilities for threat mitigation. For an event the size of the G20, the audience is large and diverse, and engaging the relevant individuals is key. Stakeholders should be grouped based on roles, and specific exercises and training should be customized for each group's responsibilities.

Through these campaigns, all individuals who are essential to securing the G20 can better understand the implications of taking certain decisions or actions, and this understanding will improve overall cybersecurity readiness. Scenarios can be identified and simulated to improve remediation of cybersecurity risks. It is especially useful to carry out cyber drills and exercises during adverse circumstances – such as the COVID-19 pandemic – as this strengthens individuals' agility to face unforeseen events.

The existence of focal points of contact and channels of communication between the NCA and the key stakeholders facilitated prompt and continuous communication, and this was integral to responding efficiently. It is important to establish and codify these channels to promote cooperation and responsiveness among key stakeholders.

Conclusion

The Kingdom of Saudi Arabia was honored to host world leaders, ministers, and delegates during its G20 Presidency in 2020 and promote the Summit's mission to achieve the opportunities of the 21st century for all. Given the multitude and diversity of its participants, as well as its duration, the G20 represents the premiere forum for international cooperation. In addition to pooling together resources, expertise, and capabilities, the G20's outcomes provide momentum for sustained coordination on issues that all our societies face.

As cybersecurity continues to receive increasing attention worldwide, its relevance has been highlighted by the need to move the vast majority of G20 events – including the Leaders' Virtual Summit – online, and to secure them.

Careful preparations for physical events had to be adapted and and re-envisioned to conform to a new digital reality. A new model was designed, building on existing plans and capabilities.

The Saudi model was built on previous experiences and on the NCA's experience and expertise in order to develop a robust model. The governance structure brought together individuals with important expertise, which was fundamental to securing the Presidency year. This was achieved by maximizing the value of existing communication channels and coordinating information sharing activities throughout the year. Roles and responsibilities were codified and operationalized in the cybersecurity operations conducted throughout the year. This included cybersecurity assessments, threat modeling and monitoring, and robust incident response. Awareness campaigns and training exercises – including cyber drills – were also used to strengthen a culture of cybersecurity across all key stakeholders. The Presidency leads up to the most important G20 event – the Leaders' Virtual Summit - where all efforts of the Saudi cybersecurity model were scaled up and reinforced.

https://nca.gov.sa/ Info@nca.gov.sa NCA_KSA