strategy&
Formerly Booz & Company

Cyber security in the Middle East

A strategic approach to protecting national digital assets and infrastructure

Strategy& is part of the PwC network

Contacts

Abu Dhabi

Samer Bohsali
Partner
+971-2-699-2400
samer.bohsali
@strategyand.pwc.com

Sevag Papazian
Senior Associate
+971-2-699-2400
sevag.papazian
@strategyand.pwc.com

Beirut

Fadi Majdalani
Partner
+961-1-985-655
fadi.majdalani
@strategyand.pwc.com

Walid Tohme
Partner
+961-1-985-655
walid.tohme
@strategyand.pwc.com

Canberra

Jeremy Lindeyer
Principal
+61-2-6279-1900
jeremy.lindeyer
@strategyand.pwc.com

Chicago

Eduardo Alvarez
Senior Partner
+1-312-346-1900
eduardo.alvarez
@strategyand.pwc.com

Mike Connolly
Senior Partner
+1-312-346-1900
mike.connolly
@strategyand.pwc.com

Dallas

Donald Dawson
Partner
+1-214-746-6500
don.dawson
@strategyand.pwc.com

Dubai
Imad Harb
Senior Associate
+971-4-390-0260
imad.harb
@strategyand.pwc.com

Düsseldorf

Jens Niebuhr
Partner
+49-211-3890-195
jens.niebuhr
@strategyand.pwc.com

Frankfurt

Rainer Bernnat
Partner
+49-211-38900
rainer.bernnat
@strategyand.pwc.com

Munich

Nicolai Bieber
Principal
+49-89-54525-0
nicolai.bieber
@strategyand.pwc.com

About the authors

Dr. Walid Tohme is a partner with Strategy& in Beirut. He is a member of the firm's healthcare and business technology practices, and has over 20 years of experience at the intersection of health and information technology. He has led a variety of programs in North America and the Middle East covering strategy, technology, and operations for healthcare providers, payors, and regulators. He leads the Big Data efforts for Strategy& in the Middle East.

Jeremy Lindeyer is a principal with Strategy& in Canberra. He is a senior member of the defense and national security consulting team, and has over 16 years of experience in cyber-security strategy, business analysis, and capability definition. He has supported several Australian federal government departments to develop new cyber strategies, capabilities, architectures, and balanced approaches to implementation.

Imad Harb is a senior associate with Strategy& in Dubai. He is a member of the firm's digital business and technology practice and the ICT resilience team, and has over 14 years of experience in information technology and management consulting. He specializes in large-scale information technology strategies, and national cyber-security and critical information infrastructure protection strategies.

Sevag Papazian is a senior associate with Strategy& in Abu Dhabi. He is a member of the firm's digital business and technology practice, and has over 10 years of experience in technology and consulting. He specializes in large-scale technology-enabled business transformations, national cyber-security strategies, and transformation governance models.

Ramzi Ghaziri also contributed to this report.

Executive summary

The continuing success of digitization initiatives among the countries of the Middle East brings with it an added and growing exposure to the risk of cyber attacks. These attacks — by other states and by increasingly sophisticated criminal rings from around the world — have the potential to derail the progress of digitization, and threaten the benefits delivered through it.

Every national government in the region is striving to create a secure digital environment, but too often these efforts are fragmented, tactical, and reactive. Moreover, they do not include the participation of all essential stakeholders. Consequently, governmental responses often lag behind the ever-evolving threat landscape, and the defensive measures taken are circumvented or exploited. A strategic approach to national cyber security is needed that follows a "CCC" framework — *comprehensive* in nature, *collaborative* by intention, and *capability-driven*.

Middle East governments can apply the CCC framework in their own national cyber-security programs. First, they should establish a centralized national cyber-security body, with a clearly defined mandate. The established body should define a national cyber-security strategy and establish the national dialogue. Afterwards, there should be a focus on building cyber-security capabilities, both preventive and reactive, and on developing the talent and capabilities on which national cyber security rests. By acting immediately on these imperatives, governments will ensure that their nations reap the full rewards of digitization, now and in the future.

Securing the rewards of digitization

Middle East countries are pursuing digitization — the mass adoption of connected digital technologies and applications by consumers, enterprises, and governments — at a rapid pace. The region's digital markets are expanding at an overall compound annual growth rate of 12 percent and are expected to be worth US$35 billion in 2015. Strategy& estimates that digitization could add as much as $820 billion to regional GDP and create 4.4 million new and much-needed jobs by 2020.[1]

Although digitization holds the potential for rich rewards, it also brings with it significant risks from an ever-evolving host of cyber threats perpetrated by cyber criminals, nation states, and cyber hacktivists. These actors have the motivation, capability, and intent to exploit the vulnerabilities created by a nation's dependence on digital technologies for commerce and government services. This sustained barrage of cyber attacks and exploitation could undermine the confidence the government, the business sector, and civil society have in digitization, derailing its progress and thereby threatening the attainment of its promised benefits.

Cyber threats are a global phenomenon and are continually developing in sophistication and impact, despite the advances in cyber-security technologies and practice. Cyber crime has evolved into well-organized networks with advanced capabilities and specialized divisions of labor. Nation states have developed unparalleled cyber exploitation and attack technologies that they are beginning to integrate into their national military capabilities.

Nation states have developed unparalleled cyber exploitation and attack technologies that they are beginning to integrate into their national military capabilities.

The resources of Middle East countries and their rapid adoption of digitization have made the region an attractive target for a wide array of cyber threats. Indeed, governments and large organizations in almost every vital sector of the region have sustained damage from cyber attacks.

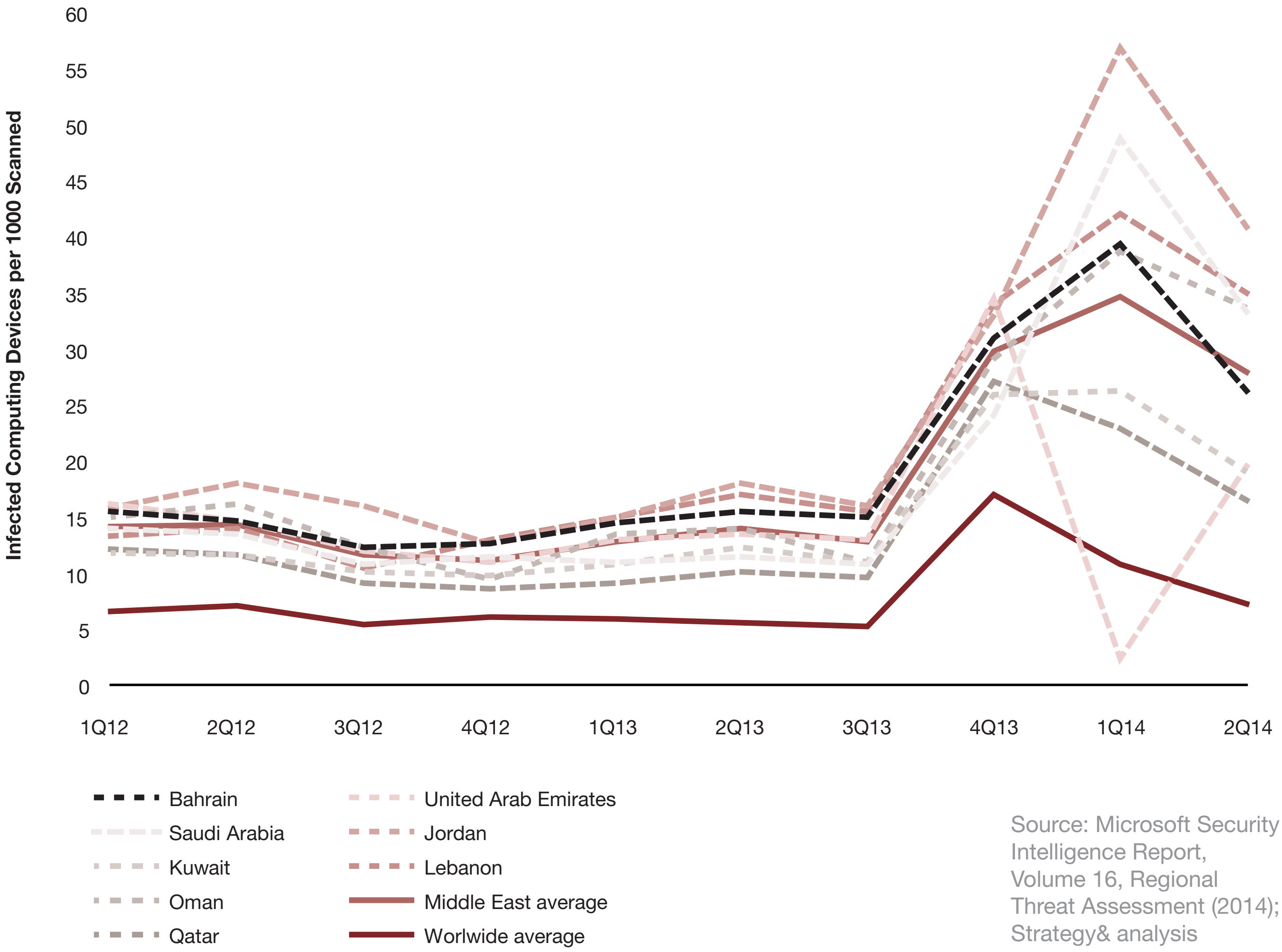
The Flame and Gauss viruses were used to conduct widespread cyber espionage, including the theft of financial information from individuals, corporations, and governments. Citadel, a financial malware variant, was used to attack the computer networks of several petrochemical companies — possibly seeking to gain access to the controls of processing plants. A malicious virus was used to breach the security of 75 percent of the computers in one of the region's major oil and gas companies. An attack on two Middle East banks resulted in a direct financial loss of $45 million in a few hours.

These are only a few examples — just the tip of the iceberg. A more telling statistic can be found in the number of virus-infected computing devices in the Middle East. It exceeds the global average by more than four-fold, a differential that has increased in recent years (*see Exhibit 1*).

Exhibit 1

Computers become infected in the Middle East at increasingly higher rates than the global average

Infected Computing Devices in the Middle East (2012–2014)



Source: Microsoft Security Intelligence Report, Volume 16, Regional Threat Assessment (2014); Strategy& analysis

The state of national cyber-security policies

Middle East governments are acutely aware of the new threat landscape associated with digitization. To bolster their national cyber-security capabilities and elevate the protection level of their critical national information infrastructures, many of them have stepped up their cyber-security activities in recent years.

Some countries have created new laws aimed at protecting electronic transactions and prosecuting cyber crimes. Others have established critical information infrastructure protection polices and cyber-security plans, and have vested responsibility for cyber security in existing agencies or directorates. Still others have initiated national incident response protocols, and have begun building cyber-security awareness and capabilities. These are all good steps toward improving national cyber security. However, these steps alone they will not suffice to manage risks associated with the digital assets of an entire country.

Most of these existing initiatives take an IT-centric approach to national cyber security. They are tactical responses to an issue that requires a strategic solution. A national cyber-security program requires a coherent, comprehensive strategy that identifies essential national cyber capabilities, and clearly assigns ownership of these capabilities and responsibility for national cyber security to a dedicated lead agency.

Most cyber-security efforts at present are reactive. Their focus is recovery from a cyber attack, as opposed to attack prevention. An effective and enduring national cyber-security program must include proactive cyber-capabilities that can help to prevent attacks, such as information sharing and continuous monitoring for elevated situational awareness.

Most current efforts focus on the role of the government in establishing and maintaining cyber security. However, a national cyber-security program must be integrative. It must involve the private sector and citizen, and enlist their assistance in addressing the protection of critical digital assets and infrastructure no matter where it is within the country.

The gap between the cyber-security capabilities of public- and private-sector entities in the Middle East and the capabilities of their adversaries in cyberspace already represents a tangible risk, and it is growing daily. To close this gap, we believe that the governments of the Middle East need to take a strategic approach to rethink and revamp their national cyber-security efforts. Until then, tactical and technical solutions to cyber attack can serve only as stopgap measures.

Three strategic imperatives

The permeable nature of the Internet — the core enabling element of a digital nation — is an impediment to securing the vast and diverse digital assets of an entire country. The Internet is borderless, allowing the launch of cyber attacks from anywhere to anywhere, at any time, by known and unknown enemies of all kinds.

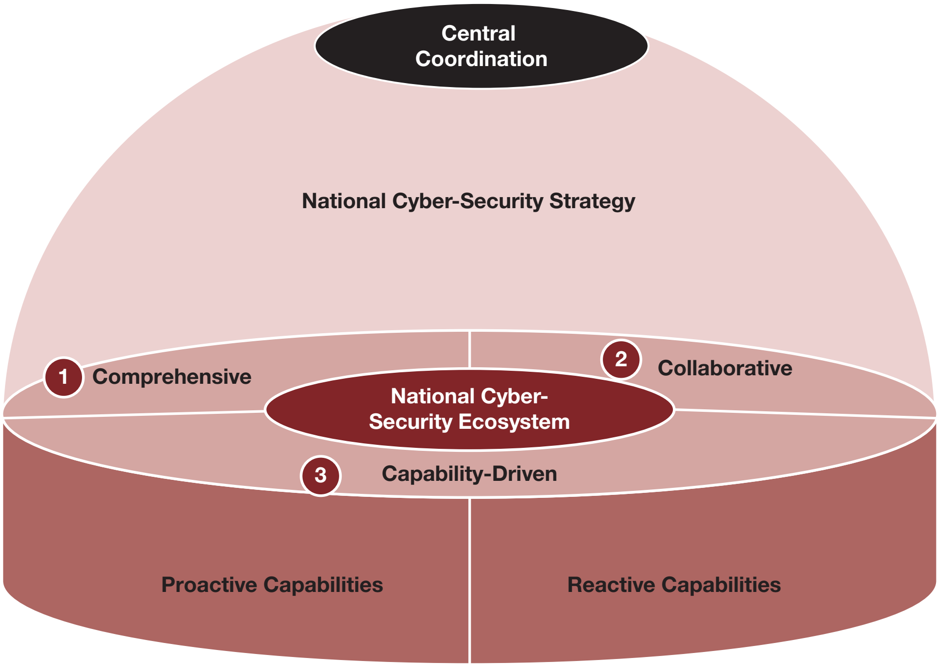
A few countries have attempted to overcome this barrier by creating a domestic cyber network that replaces the Internet within their borders — a sort of national Internet in which access is fully controlled and monitored by the government, as in the case of Myanmar in 2007, Egypt during the 2011 protests, Libya in 2011, and more recently Syria during the civil war. None have succeeded in this ultimately futile and potentially self-defeating approach. The greatest strength and the greatest danger of the Internet is that it is largely a supranational entity that defies state control. A country cannot fully capture the benefits it offers without exposure to its risks.

Thus, the only truly viable solution is a national cyber-security program, which aims to manage the risks inherent to digitization in a way that deters attacks whenever possible, and responds in a timely and effective manner to attacks that cannot be deterred. There are three strategic imperatives for such a program: It must be comprehensive in nature, intentionally collaborative, and capability-driven, hence our CCC framework (*see Exhibit 2*).

1. Comprehensive in nature: An effective national cyber-security program must encompass not only government, but also the private sector and citizens. Ensuring the cyber security of a country is a complex undertaking that requires the consideration of many aspects,

Exhibit 2

The strategic imperatives of national cyber security



1 Comprehensive

Identify and engage all aspects and players of the cyber-security ecosystem

2 Collaborative

Ensure that digital asset protection is a shared responsibility of the private sector, public sector, and citizens

3 Capability-Driven

Build both reactive capabilities and proactive capabilities that enable the prevention and deterrence of cyber attacks

Source: Strategy&

the involvement of a host of governmental and private stakeholders, and the alignment of a wide array of elements. This explains why piecemeal approaches do not work. Typically, these haphazard attempts at cyber security do not recognize all of the risks to which a country is exposed. As a result, tactical solutions can actually create gaps in cyber security, which inevitably are exploited by cyber criminals. Over the past few years, we have seen that all sectors are exposed in the Middle East, including:

- The public sector — 19 United Arab Emirates (UAE) government websites were targeted in July 2014, according to the Telecommunications Regulatory Authority (TRA) of the UAE
- Oil and gas — Saudi Aramco and RasGas, the Qatari national gas producer, fell victim to attacks in 2012
- Financial services — RAK Bank in the UAE and BMI in Oman were attacked in 2012 and 2013, respectively, by an international group of hackers

To avoid this, a strategic approach to national cyber security seeks to identify all aspects and players of the cyber-security ecosystem. Such an approach should include the following three elements:

- Identifying the key private and public stakeholders who should take part in the national cyber-security program, and their roles in collectively driving this effort
- Establishing the needs of each stakeholder and addressing these needs in a holistic cyber-security program
- Creating an integrated planning and implementation approach for individual national cyber-security initiatives aimed at ensuring the participation of all stakeholders

Tactical solutions can actually create gaps in cyber security, which inevitably are exploited by cyber criminals.

2. Intentionally collaborative: The strategic approach to cyber security is based on the hard reality that it is not possible to defend all of a country's digital assets without the collaboration and integration of all of the primary stakeholders from the private and public sectors, and citizens using the nation's digital networks. Private companies can be targeted by state entities and may need support from their own state. For example, the Sony hack in late 2014 appears to have involved a state actor targeting a commercial organization. Accordingly, collaboration between governments, commercial institutions, and individuals will become of paramount importance in the future. However, this is a long journey. As President Barack Obama said in his speech at the National Cybersecurity Communications Integration Center in January 2015, "Sometimes it's still too hard for government to share threat information with companies.

Sometimes it's still too hard for companies to share information about cyber threats with the government. There are legal issues involved and liability issues. Sometimes, companies are reluctant to reveal their vulnerabilities or admit publicly that they have been hacked."[2]

Ensuring the protection of digital assets is a shared responsibility that requires action at many levels. Although strong leadership is critical to national cyber security, sector regulators, government, private-sector entities, and the national and international community at large also have essential roles to play. Integrative alignment and collaboration enable a country to leverage its existing cyber-security strengths and to catalyze the implementation and adoption of new cyber-security measures. To achieve this, the four following elements must be addressed:

- Establishment of shared operational responsibilities with relevant stakeholders in the private sector. Sector regulators can play an important role in this regard by driving the development of sector-specific cyber-security requirements and information infrastructure protection plans aimed at elevating security and cyber capabilities within sectors.
- Engagement and enablement of citizens and communities so that they can shoulder their share of responsibility for national cyber security. The national workforce and the public at large must become more aware, through training and information campaigns, of the basics of cyber security as they pertain to the protection of their own interests from the threats and the techniques that could be employed against them.
- Advocacy for a regional body to share responsibility for cyber security across the Middle East. This coordinating body should develop cyber-security capabilities designed to protect the increasingly connected economies, societies, and national interests in the region.
- Fostering of collaboration between national and international stakeholders to create a cyber-security environment in which information, best practices, and lessons learned are shared and widely adopted.

A hallmark of a strategic approach is that it includes both reactive capabilities and proactive capabilities that enable the prevention and deterrence of cyber attacks.

3. Capability-driven: The ability to respond quickly and effectively to cyber attacks, although an important component of a national cyber-security program, is not enough to protect a country's digital assets and infrastructure. A hallmark of a strategic approach is that it includes both reactive capabilities and proactive capabilities that enable the prevention and deterrence of cyber attacks.

A world-class cyber-security program must provide proactive protection by addressing the following three elements:

- Development and nationwide adoption of information assurance standards that are designed to elevate the resilience of country's critical cyber assets and reduce corresponding risk levels
- Regular and ongoing measurement and testing of national cyber-security capabilities to identify exploitable weaknesses and gaps and develop mitigation plans
- Assurance that cyber security is considered as a component in the decision making and daily activities of the government, the private sector, and citizens

Knowing that not all cyber attacks can be prevented, reactive capabilities should be in place that include:

- Planning for worst-case scenarios to ensure optimal reaction and recovery from a cyber attack in coordination with local and international players
- Development of a national incident capability that enables response to, and recovery from, cyber attacks in a manner that reduces their impact on society and the economy
- Establishment of threat neutralization and cyber law enforcement capabilities that protect citizens, the private sector, and the government from cyber criminals.

In support of both proactive and reactive capabilities, a national cyber-security program should include the development of the offensive and defensive cyber capabilities needed to neutralize and respond to cyber warfare and enhance national security. It should encompass the monitoring of the threat landscape through a national situational awareness capability that is supported by an information-sharing platform and model that supports cyber threat intelligence capabilities. Moreover, it should promote cyber-security research and innovation, and the development of the talent required to meet national cyber-security needs.

In the U.S., for example, the cyber-security framework released by the National Institute of Standards and Technology in February 2014 addresses five major cyber-security functions (identify, protect, detect, respond, and recover) that cover the gamut of proactive and reactive capabilities. In the U.K., the Cyber-security Information Sharing Partnership (CISP), a broadly based government–industry partnership, was launched in 2013 to share information and intelligence on cyber threats. It includes “a secure virtual ‘collaboration environment’ in which government and industry partners can exchange information on threats and vulnerabilities in real time,” and will be supported on the government side by the Security Service, the Government Communications Headquarters (GCHQ), and the National Crime Agency, and by industry analysts from a variety of sectors.[3]

In addition to our CCC framework, a strategic approach to national cyber security should involve centralized control. To elevate the accountability of cyber security to the highest level and to ensure it is treated as a national priority (as opposed to only an IT concern), a lead cyber-security entity should be established at the country level. This authority would be responsible for determining cyber-security strategy, and for creating and implementing the national policies and standards, governance structures, ownership models, macro roles and responsibilities, and cyber-security capabilities on which a national program is built.

A strategic approach to national cyber security should involve centralized control.

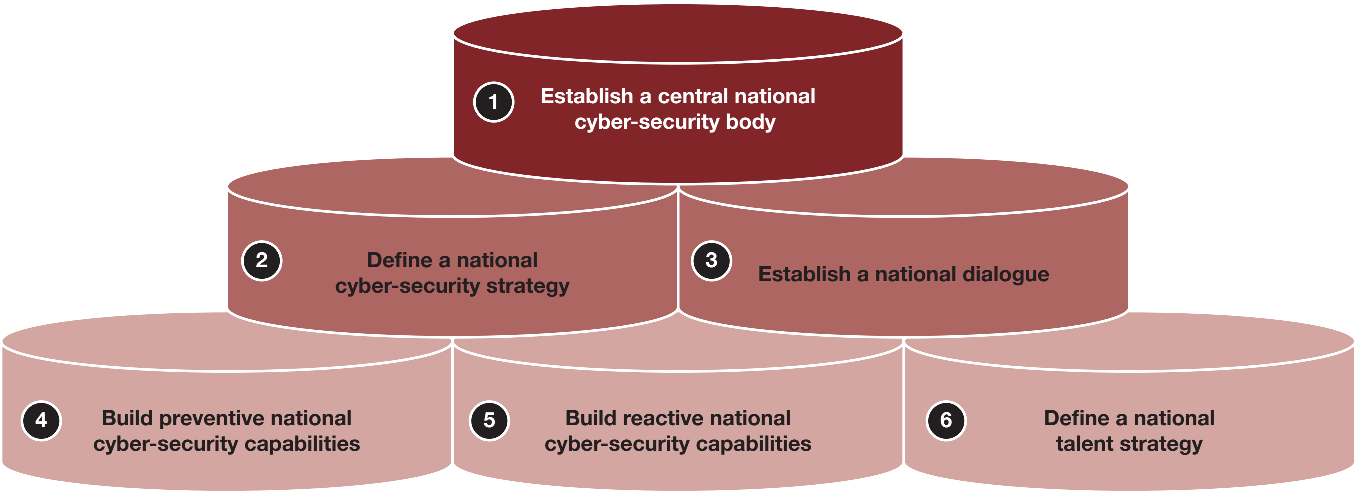
A practical approach for the Middle East

The establishment of a safe and secure environment for existing and future digitization initiatives in the Middle East is a challenging undertaking that we believe must begin at the national level with a strategic approach to developing a comprehensive cyber-security program that follows the CCC framework. Such a program must be governed by a dedicated authority and enlist the commitment, effort, and resources of all of its stakeholders to deter proactively and respond effectively to cyber attacks.

In this regard, the national governments of the Middle East have specific considerations that do not always hold true outside the region. For instance, the close ties between government and major industries — and the public initiatives that drive sector development (such as the Tawazun Holding economic program in the United Arab Emirates) — offer a leg up on the strategic imperative of collaboration. Conversely, the dearth of homegrown talent creates obstacles to standing up essential cyber-security capabilities and thus, executing a national strategy. With the unique considerations of the Middle East in mind, we recommend six initial steps that governments should undertake in the adoption and implementation of their cyber-security programs (*see Exhibit 3*).

Exhibit 3

A practical approach to national cyber security


1 Establish a central national cyber-security body
2 Define a national cyber-security strategy
3 Establish a national dialogue
4 Build preventive national cyber-security capabilities
5 Build reactive national cyber-security capabilities
6 Define a national talent strategy

Source: Strategy& analysis

1. Establish a central national cyber-security body: The national government should establish a central national cyber-security body (CNCB) responsible for defining and supervising the national cyber-security agenda. It is imperative for this entity to be independent and not part of any existing public organization, such as ministries, councils, or regulatory authorities. This will ensure the impartiality of the body, which is the key to eliminating any lack of cooperation from a group of stakeholders and ensuring collaboration. At the same time, this newly created body has to be empowered by the highest authorities, such as the national security council, and officially mandated through laws or decrees, to ensure its credibility and give it sufficient authority vis-à-vis public and private organizations.

2. Define a national cyber-security strategy: The CNCB should create a national cyber-security strategy that is aligned with the country's vision, national interests, and national/regional security imperatives. As mentioned earlier, the strategy should be comprehensive, collaborative, and capability-driven. One of the key success factors of the strategy is the full involvement of key national stakeholders throughout the process of developing the strategy, to ensure that key ideas and elements are reflected in the strategy. This approach is preferable to the one that some authorities take of developing a strategy in silos, which makes it very difficult to socialize the strategy and obtain stakeholder support.

The strategy should be comprehensive, collaborative, and capability-driven.

3. Establish a national dialogue: The CNCB should establish the national dialogue across key stakeholders to start the collaboration process. This dialogue can take the form of a national cyber-security governance body chaired by the CNCB, through working groups that focus on specific topics or industries, or through regular conferences and other events.

4. Build preventive national cyber-security capabilities: The CNCB should take the lead in building preventive national cyber-security capabilities. This includes the development of national cyber-security standards and policies, such as a national information assurance standard. It also includes establishing a national compliance body that ensures the implementation of such standards and policies.

5. Build reactive national cyber-security capabilities: The CNCB should also drive the establishment of reactive national cyber-security capabilities. This includes the establishment or empowerment of a national Computer Emergency Readiness Team. Because in most countries such organizations already operate in one shape or another, it is imperative to align the strategic direction of the Computer Emergency Readiness Team with the national cyber-security strategy. This leverages the power of collaboration to define the types of responses that the country wants to build.

6. Define a national talent strategy: Attracting talent within the cyber-security space is inherently challenging. This task is particularly difficult in most emerging markets, including the Middle East. To increase interest in cyber security both organically and inorganically, individuals, and especially students, should be incentivized to join the industry. This requires establishing clear cyber-security curricula in national and regional universities, in alignment with government and commercial organization requirements. Experts should be attracted through collaboration programs with international organizations and with attractive financial packages. Finally, nations in the region should host world-class forums to raise awareness and interest at a national and regional level. Some of the Middle East countries that already have a national talent strategy should incorporate cyber security within their existing talent development agendas.

Conclusion

The governments of the Middle East are the only stakeholders with the power, reach, and resources necessary to develop and drive a truly national cyber-security agenda, to ensure alignment of efforts, and to drive collaboration and continuous improvements through sector-specific, national, and ultimately regional governance bodies. This is why it falls to government to define a national cyber-security program, assign ownership and responsibility at the highest level, and launch the program. All that remains is for Middle East leaders to address this critical problem, which threatens their national digitization efforts and prospects for viable, twenty-first century economies.

Endnotes

[1] See "Accelerating digitization in the Middle East: 2012 ICT leaders' event," Strategy&, 2013 (http://www.strategyand.pwc.com/media/file/Accelerating-digitization-in-the-Middle-East.pdf).

[2] President Barack Obama, "Remarks by the President at the National Cybersecurity Communications Integration Center," The White House, Office of the Press Secretary, January 13, 2015 (http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent).

[3] The Cabinet Office and The Rt Hon Francis Maude MP, "Government launches information sharing partnership on cyber security," March 27, 2013 (https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security).

Strategy& is a global team of practical strategists committed to helping you seize essential advantage.

We do that by working alongside you to solve your toughest problems and helping you capture your greatest opportunities.

These are complex and high-stakes undertakings — often game-changing transformations. We bring 100 years of strategy consulting experience and the unrivaled industry and functional capabilities of the PwC network to the task. Whether you're charting your corporate strategy, transforming a function or business unit, or building critical capabilities, we'll help you create the value you're looking for with speed, confidence, and impact.

We are a member of the PwC network of firms in 157 countries with more than 195,000 people committed to delivering quality in assurance, tax, and advisory services. Tell us what matters to you and find out more by visiting us at strategyand.pwc.com/me.

www.strategyand.pwc.com

Disclaimer: This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.