Microsoft

Building an effective national cybersecurity agency

Authors

Paul Nicholas
Kaja Ciglic

Contributors

Theo Moore
Jessica Zucker
Angela McKay
Jan Neutze

Cybersecurity: New thinking required

Cybersecurity is top of mind for governments, enterprises, civil society and consumers. Every day there is news of a new cyber-attack, a new cybersecurity legislation or regulation proposal, or a new vulnerability in technology platforms that needs to be addressed. Every aspect of society is increasingly participating in a global dialogue focused on these issues.

Microsoft is an active participant in all aspects of this dialogue. For over twenty years we have not only invested heavily in the cybersecurity of our products and services, from Windows to Xbox to Azure, but we have also contributed to the security of the broader online ecosystem. We took what we learned from improving the security of our systems and made those lessons broadly available through international standardization processes, for example with the Security Development Lifecycle. We have also continuously shared threat, vulnerability, and remediation information with governments and partners around the world to ensure they can quickly and appropriately defend against or respond to any potential attacks.

Our commitment goes beyond solving technical problems and innovating new defenses. Last year we challenged governments with our proposal promoting a Digital Geneva Convention. We believe international law needs to evolve and be applied more vigorously, so that we can limit the increasingly aggressive and destabilizing behavior of nation states in cyberspace. Our Digital Crimes Unit has similarly been driving applications of existing domestic laws around the world to protect our customers from cybercriminals. Those cases have allowed us to take down some of the largest international botnets and bring their creators to justice, as well as yielded valuable data for our engineers to use in solidifying the security defenses of our products and services.

This paper reflects yet another aspect of Microsoft's engagement on cybersecurity: working with policy makers and legislators around the world to share our understanding of which cybersecurity policy approaches have proven to be effective. In doing so, my team harnesses methods that have been tried and tested within Microsoft and then adapts them to broader frameworks so that they can be adopted at a national level in a technology neutral way. They also draw on Microsoft's experience as a global company, allowing us to observe and adapt our proposals to government actions across different cultural and technical backgrounds.

The proposals included here build on the "Developing a national cybersecurity strategy" white paper, which for the first time identified cybersecurity as an issue that needs comprehensive action at the national level. Since then more than 80 countries have adopted national cybersecurity strategies and begun to implement them. That experience has led many countries to conclude that an effective implementation is only possible with a strong coordinating central authority or agency.

The governance of these authorities varies, depending on national legislative frameworks and levels of cybersecurity expertise. With this paper we do not seek to impose a single model, but to put forward good practices that allow governments to achieve their cybersecurity goals more easily and sustainably. As the challenges and opportunities related to the proliferation of technology continue to grow and evolve, policy approaches and structures will have to be flexible. I hope that this paper contributes to the ongoing dialogue and to a safer online environment for us all.

Tom Burt, Vice-President, Deputy General Counsel, Digital Trust, Microsoft

Contents

Introduction

Information and communication technology (ICT) has been firmly established as a pillar of modern life. Continuous and rapid innovation has resulted in a profound digital transformation of social, economic, and government frameworks. It has brought numerous benefits, from increased effectiveness and productivity, to easier access to information and learning. However, it has also exposed increasing numbers of individuals, businesses, and governments to new threats.

Governments have an important role to play in responding to those threats, and ensuring the security of their citizens, offline as well as online. To help do so, they have increasingly sought to develop cybersecurity approaches at national levels, by adopting various national cybersecurity strategies, polices, laws, and regulations. However, the cross-cutting nature of cybersecurity does not fit neatly into established governance frameworks and many have struggled with developing comprehensive and effective approaches.

Depending on the levels of cybersecurity maturity, as well as the overall national governance framework, the mandate for dealing with cybersecurity has been given to different government bodies, each with more or less responsibility and power to affect change. In some countries, cybersecurity has become the responsibility of dedicated departments within particular ministries (e.g. ministry for ICT or defense) or an extension of the work done by the police force or by the national computer security incident response teams (CSIRTs). On many occasions it has resulted in the establishment of a standalone body: a national cybersecurity agency.

There is a growing belief that a standalone national cybersecurity agency, if appropriately structured, can substantially increase the readiness of a country's cybersecurity ecosystem. However, while many countries already have some type of national cybersecurity body in place, it can be observed that these frequently get restructured, as governments continue to search for an optimum way to manage a relatively new, but critical, area of governance. While the search for improvement is constant, with this white paper Microsoft seeks to offer a set of observations and good practices to help guide policymakers in these endeavors. The recommendations in terms of structure, roles, and responsibilities included in the document, stem from Microsoft's interactions with government agencies around the world. We are also drawing on what we have learned as an organization that has to effectively respond to cybersecurity incidents and establish partnerships with governments, customers and peers.

National cybersecurity agency: Differing approaches and structures

Cybersecurity has become a national priority for the majority of countries around the world and rightly so. Over the last two decades, billions have benefited from economic and social opportunities driven by the exponential growth and rapid adoption of ICT. That same development has, however, also given rise to new cyber-threats, from fraud and theft of intellectual property or personal data, to the disruption of services, and even destruction of property. Ensuring the confidentiality, integrity and availability of this new technological infrastructure in the face of constantly evolving cyber-threats has become a necessary government priority.

Today, many governments[1] are working to adopt, review, or implement national cybersecurity strategies, policies, laws, regulations or other national approaches, with countless other efforts taking place at sectoral, state, city or other levels. To support the implementation of these, certain countries have considered the development of a central cybersecurity agency or a similar body to help manage their cybersecurity priorities. Countries as diverse as Australia, France, Tanzania, Belarus, Israel, and Singapore, to name a few, already have specific bodies responsible for cybersecurity in place.

However, developing effective approaches to tackling cybersecurity at national level isn't easy, especially if they are going to have widespread or long-lasting effects. The task of such agencies is therefore complex; not just because of the pervasiveness of computing today, but because of the legacy of pre-cyber policy-making and regulation. Effectively, cybersecurity is one of the first policy areas that challenges traditional governance structures and policy-making. National cybersecurity approaches need to tackle a great deal, from promoting online safety and protecting government services and critical infrastructures, to engaging internationally to tackle global threats. These topics cut across an unprecedented range of traditional government departments, from defense and foreign affairs, to education and finance.

Effectively, cybersecurity is one of the first policy areas that challenges traditional governance structures and policy making.

Similarly, a siloed approach is reinforced by traditions of sectoral regulation for other areas of policy-making. That can mean sectors governed by strong regulators, such as financial services or energy, having firm but differing cybersecurity rules, whilst other less regulated sectors having no rules at all. The challenge is that a sectoral or vertical approach does not accord with the cross-cutting, horizontal nature of the technology and of cybersecurity good practices, where a weakness in one area can easily translate into a weakness for all. For a national cybersecurity agency this inheritance of departmental and sectoral difference can complicate determining the necessary common baselines for cybersecurity.

Moreover, governments are particularly dependent on the private sector when it comes to dealing with cybersecurity. The majority of online infrastructure is owned and operated by the private sector, which therefore holds much of the information related to cybersecurity threats. As a result, the effectiveness of national cybersecurity approaches often hinges on how successfully and how extensively the private sector is involved in awareness raising, information exchange, and policy development.

[1] Microsoft's internal research shows that over half of all countries are - as of October 2017 - developing cybersecurity policies, strategies, law or regulations

Microsoft
Building an effective
national cybersecurity agency

Those national cybersecurity agencies that have already been established to help navigate this complex environment vary in terms of structure and responsibility.[2] A smaller number of governments have established standalone cybersecurity authorities and have given them responsibilities across the spectrum of cybersecurity issues (for example, Singapore[3]). Others have established several organizations, each dealing with a specific aspect of cybersecurity, e.g. assurance, incident response, awareness raising (for example, United Kingdom,[4] or the Netherlands[5]). Another approach has been not to establish new authorities or organizations but to rely on a central coordination body or committee to manage the numerous cybersecurity roles and responsibilities dispersed across different government departments (for example, Italy[6]). Such bodies or committees tend to primarily coordinate internal government efforts rather than focus externally, leaving many international or private sector stakeholders to deal with several interlocutors.

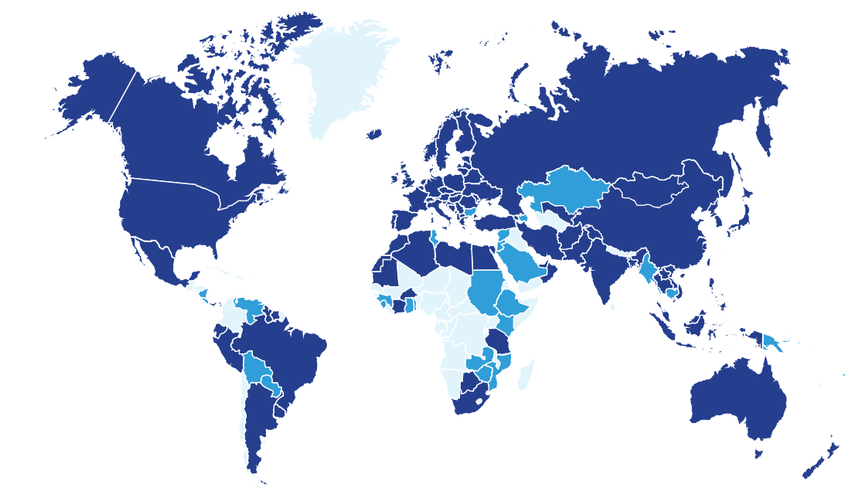
Those national cybersecurity agencies that have already been established to help navigate this complex environment vary in terms of structure and responsibility.

National cybersecurity agencies, even if technically standalone or reporting to the highest levels of government, often sit within a particular ministry or department, depending on where the primary responsibility for cybersecurity falls.[7] The selection of the relevant ministry or department often stems from how the country sees cybersecurity. It can for instance be perceived as part of the innovation economy and therefore sits in the ministry of ICT (for example, India[8]). Alternatively, it can be seen as an extension of the e-government work and therefore be housed in the ministry of finance or administration (for example, Slovakia[9]). Moreover, cybersecurity can be interpreted as part of traditional security policy and thus the responsibility of intelligence services or the ministry of defense (for example, Lithuania[10]).

Finally, it is worth noting that many governments have allowed their approaches and agencies to evolve gradually over time rather than creating them in one fell swoop. Some have begun with a smaller organization embedded within a particular government department that has later scaled to become a dedicated standalone authority (for example, Israel[11]). Others have gradually elevated the roles and responsibilities of the existing group to ensure it can effectively perform its functions (for example, Slovenia[12]). The evolving nature of national cybersecurity approaches should not be taken as an indicator of a lack of maturity. Rather it should be seen as a positive recognition of the fact that effective cybersecurity risk management, at any level, requires continuous learning and evolution in the face of constantly developing cyber-threats and rapidly developing technology.

[2] Although structure of governmental bodies responsible for cybersecurity will inevitably differ across countries, we refer to them in general terms as "national cybersecurity agencies". Furthermore, for the purposes of this white paper, we focus solely on the civilian aspects of cybersecurity and do not include the military or intelligence aspects of cybersecurity.
[3] Cyber Security Agency of Singapore: https://www.csa.gov.sg/
[4] CCD COE: National Cybersecurity Organization – United Kingdom: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf
[5] CCD COE: National Cybersecurity Organization – the Netherlands: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf
[6] CCD COE: National Cybersecurity Organization – Italy: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ITALY_032015_0.pdf
[7] Map is based by the research conducted by the International Telecommunications Union as part of their Global Cybersecurity Index, 2017: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
[8] Indian Ministry of Electronics and Information Technology: http://meity.gov.in/
[9] CCD COE: National Cybersecurity Organization – Slovakia: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SLOVAKIA_042015.pdf
[10] CCD COE: National Cybersecurity Organization – Lithuania: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf
[11] CCD COE: National Cybersecurity Organization – Israel https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf
[12] Slovenian national body for cybersecurity: http://www.uvtp.gov.si/si/medijsko_sredisce/novica/article/335/1360/

MAP: Countries with established or developing a national cybersecurity agencies[13]



2= Has National cybersecurity agency;
1= Agency under development

[13] Based on ITU Global Cybersecurity Index (GCI) 2017, question: Is there a national body/agency responsible for cybersecurity?
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Structuring an effective national cybersecurity agency

Allowing for many different forms that a national cybersecurity agency can take, Microsoft's experiences of working with governments around the world indicate that there are some particularly effective approaches to structuring them. These span the operational structure of an agency, as well as its roles and responsibilities.

In this section, we put forward five recommendations that bring together good practices from around the world. In doing so we propose a conceptual structural model for a national cybersecurity agency, as well as outline the roles and responsibilities that it would need to have to deliver on its objectives. While this paper is agnostic as to who in the government should handle issues related to cybersecurity, recognizing the reality that this choice largely depends on the existing national governance framework, experience shows that the private sector and civil society are often more willing to engage with civilian agencies rather than security, intelligence or military bodies, not least because private sector co-operation with those agencies that might be involved in offensive cyber operations remains a particularly sensitive and challenging topic. As indicated at the outset, the former are therefore the focus of this paper.

The five recommendations for structuring an effective national cybersecurity agency are:

1. Appoint a single national cybersecurity agency
2. Provide the national cybersecurity agency with a clear mandate
3. Ensure the national cybersecurity agency has appropriate statutory powers
4. Implement a five-part organizational structure
5. Expect to evolve and adapt

1 Appoint a single national cybersecurity agency

A single agency dedicated to managing cybersecurity at the national level can be an effective way for managing the security of civilian agencies, critical infrastructure protection and national level incident response. Governments have limited time, expertise and resources to deal with the range of threats they face. Bringing core national level functions for coordination, standards setting, incident response, partnership and international outreach into one agency will allow governments to prioritize their limited resources. In addition, having a single agency that facilitates such coordination also ensures that agencies do not duplicate efforts. Some governments may choose to leave expertise distributed across government agencies but establish a clear leader and coordination process – in essence a virtual agency to increase accountability and unify efforts.

As cybersecurity concerns cut across many "traditional" policy and regulatory silos, such as justice, treasury, defense or foreign affairs, having a cybersecurity agency that can support the other relevant agencies with their particular challenges, will improve effectiveness of government-wide cybersecurity. In contrast, fragmentation may well see different cybersecurity teams spread across various departments and/or agencies making divergent decisions and taking different approaches, which will inevitably create weaknesses that attackers can exploit.

However, managing across the many silos of government, the agency must be more than a single point of reference; it must have the support of national leadership. Access to the highest levels of government is also required; the mere fact that a national cybersecurity agency has the endorsement and attention of those immediately around a prime minister or president can help ensure the intra-departmental commitment and support it requires to succeed. In line with this, it is also important that government agencies or departments with some responsibility for managing cybersecurity for the country are identified and that mechanisms for coordination and cooperation between them and the national cybersecurity agency are established. In practice, this can mean relevant ministries embedding cybersecurity functions within themselves in order to liaise with a standalone national cybersecurity agency.

Good practice: Cyber Security Agency Singapore (CSA)[14]

CSA is the national cybersecurity agency of Singapore, established in 2015. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information.

CSA consolidates and builds upon the government's cybersecurity capabilities, including strategy and policy development, cybersecurity operations, industry development and outreach. It also works closely with the private sector to develop Singapore's cybersecurity policy ecosystem.

[14] https://www.csa.gov.sg/

2 Provide the national cybersecurity agency with a clear mandate

Any national cybersecurity agency will be expected to navigate a complex environment that spans other government departments, national legislatures, established regulatory authorities, civil society groups, the general public, public and private sector organizations, and international partners. These interactions will range from policy setting and information sharing to managing the aftermath of cyber-attacks. It is therefore important that all stakeholders have a clear expectation of what the mandate of the national cybersecurity agency is, so they know what to expect and who the primary points of contact are.

It is also critical that the responsibilities of the national cybersecurity agency are distinct from those of other governmental groups touching on cybersecurity. One such example are regulators in critical infrastructure sectors, such as financial services, power generation or transport, which can set security policies for their industry in some contexts. Another example are data protection authorities, whose work can overlap with cybersecurity efforts. It is therefore important that not only are the mandates of the different agencies distinct, but that all stakeholders have a precise understanding of who is responsible for what, and of where authority is assigned in any relevant policies, laws and regulations.[15]

Good practice: Cybersecurity Agency of France (ANSSI)

ANSSI was established as France's main cybersecurity authority in 2009 with Decree No. 2009-834. Its powers have been further expanded with the 2013 Military Programming Law. Its mandate includes, among other things:

- Improving national cybersecurity capabilities by training government cybersecurity personnel;
- Provision of expertise to relevant ministries on the security and integrity of the critical infrastructure sectors and government networks;
- Setting and overseeing the implementation of cybersecurity standards;
- Coordination or incident response and threat information exchange, including through the French CERT;
- Law enforcement support in cybersecurity investigations;
- International coordination on cybersecurity;
- Authorization of electronic signatures and cryptography services.

[15] ANSSI https://www.ssi.gouv.fr/en/

In practice, the most effective approaches involve the national cybersecurity agency being responsible for:

- Overseeing implementation of the national cybersecurity strategy;
- Developing cybersecurity policies and guidelines;
- Improving national cybersecurity capabilities by overseeing cybersecurity risk assessments and management for government entities and critical infrastructures;
- Reducing the vulnerability of critical systems and networks by developing and implementing minimum cybersecurity baselines[16] and requirements for those sectors;
- Overseeing incident response, incident assistance and crisis management, typically via a national Computer Emergency Response Team (CERT) whose primary functions typically reside within the agency;
- Directing research and development into cybersecurity at national level, and managing the national cybersecurity workforce pipeline;
- Encouraging the development of a local cybersecurity ecosystem by providing specific incentives, creating incubators, etc.;
- Nurturing relationships with civil society and the private sector;
- Providing cybersecurity awareness raising, education and outreach;
- Establishing and maintaining cooperative relationships with international partners.

[16] Security baselines are a foundational set of policies, outcomes, activities, practices, and controls intended to help manage cybersecurity risk.

3 Ensure the national cybersecurity agency has appropriate statutory powers

Currently, most national cybersecurity agencies are established not by statute but by delegating existing powers from other parts of government. For example, Singapore's Cyber Security Agency was established as part of the Prime Minister's Office, and is managed by the Ministry of Communications and Information. This is consistent with the current approach in most other jurisdictions that have a national cybersecurity agency.

We anticipate that this approach will begin to shift, however, as more and more governments pass comprehensive cybersecurity laws. In the same way that the passage of comprehensive data protection laws led to the establishment of specific bodies to enforce the relevant laws, such as the Australian Information Commissioner Act[17] and the data protection legislation[18] in Europe, the enforcement of comprehensive cybersecurity laws may come to require the establishment of specific cybersecurity bodies, such as a national cybersecurity agency.

The underlying driver for this evolution is that the delegation of existing powers, subject themselves to multiple underlying laws and regulations, may not be sufficient to provide the national cybersecurity agency with all of the powers it requires to effectively carry out its new functions. Furthermore, a level of clarity might be required as to which authorities and which legislative initiatives take precedence in certain circumstances. The draft Singaporean cybersecurity bill, published in summer of 2017, is likely to be the forerunner of many of such initiatives.[19]

Principles to guide statutory measures to establish a national cybersecurity agency

- **Risk-based and proportionate.** The agency should seek to manage the cybersecurity environment via a proportionate, risk-based framework that enables organizations to innovate and adopt new technologies without exposing the country to unnecessary cybersecurity risks.
- **Outcome-focused.** It is essential that the agency focuses on delivering the desired end state, rather than prescribing the means to achieve it, and then measure progress towards that end state.
- **Prioritized.** Not all threats are equal. The national cybersecurity agency should adopt a graduated approach to criticality, prioritizing critical infrastructure risks.
- **Practicable and realistic.** Cybersecurity policies are of little value if they impose undue burdens on the organizations who must comply with them. Engagement with industry is a necessary first step to ensuring that policies are practicable and realistic.
- **Respectful of privacy, civil liberties, and rule of law.** Enforcing cyberspace cannot come at a cost of sacrificing privacy, civil liberties, and rule of law. Instead, a balanced approach is needed that is respectful of these fundamental principles.
- **Globally-relevant.** The national cybersecurity agency should leverage international standards to the maximum extent possible. Cybersecurity is a problem that transcends territorial boundaries and it is important that the country does not take steps that may limit its ability to collaborate with international partners.

[17] Australian Information Commissioner Act: https://www.legislation.gov.au/Details/C2010A00052
[18] European Union Data Protection legislation: http://ec.europa.eu/justice/data-protection/
[19] Draft Singaporean Cybersecurity Bill, 2017: https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en

4

Implement a five-part organizational structure

From experience of both working with governments and their various agencies and analyzing examples of national cybersecurity agencies across the world, Microsoft has compiled a set of good practices for structuring and organizing an agency. Based on this, an ideal national cybersecurity agency would be composed of five component parts, as outlined in the figure below, each having a specific mandate but working in collaboration with the others:

- Policy and planning unit;
- Regulatory unit;
- Outreach and partnership unit;
- Communications unit;
- Operations unit / Computer emergency response team.

This five-part structure allows for a multifaceted interaction across internal government and regulatory stakeholders and external stakeholders from the public and private sectors, as well as the international arena. In particular, it addresses one of the core challenges governments have faced in establishing national cybersecurity agencies: how to reconcile mandatory reporting of cyber-incidents, as handled by the Regulatory unit, with the voluntary and bi-directional exchange of information about cyber-threats and -incidents, as handled by the CERT. It does so by placing the Regulatory unit and the CERT within the same structure and then creating policy controls that control the flow of data between the two.

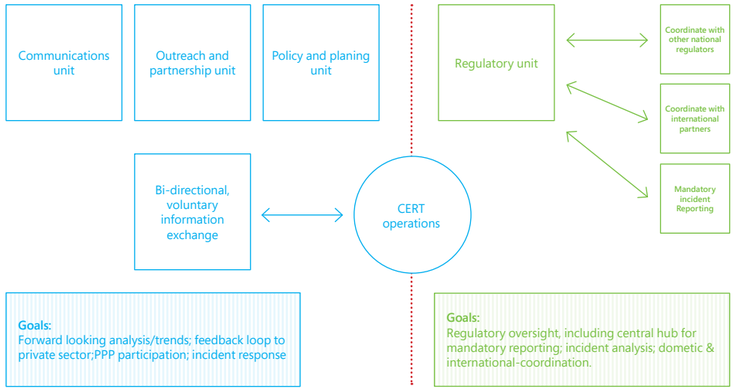


Figure 1:
High-level concept for a modern cybersecurity agency

Policy and planning unit

The Policy and planning unit should lead the development, coordination, alignment, and integration of cybersecurity policies, strategies and plans for the country. It should define near-, mid-, and long-term strategic priorities, and develop plans to implement those priorities. These priorities should include actions, milestones and budget proposals, and the unit should track and monitor progress against these plans. In the process of doing so, the unit is likely to produce and/or update a national cybersecurity strategy or policy document every few years.

The Policy and planning unit represents the government's cybersecurity policy priorities in interactions with other relevant national stakeholders, with similar policy teams from other countries, and with foreign government officials or international organizations. To be able to achieve these goals and to ensure policies are technically feasible and actually advance security objectives, the unit must be composed of personnel with a diverse set of expertise, such as in public policy, law, and engineering.

Some of the activities this unit could undertake include:

- Developing policies and strategies to improve the resiliency and security of critical infrastructure;
- Drafting or advising relevant authorities on regulatory policy for cybersecurity issues;
- Developing horizontal baseline security practices across all government departments and agencies and critical infrastructures;
- Developing policies that facilitate the voluntary sharing of information between the private sector entities and the CERT;
- Establishing clear definitions and thresholds of cyber-incidents, as well as objectives in order to develop effective incident response frameworks;
- Driving alignment of international standards, regulations, and voluntary frameworks, i.e. NIST Cybersecurity Framework[20];
- Engaging with the CERT and relevant technical security agencies to understand strategic changes in threat and risk environment and work with the communications team to raise awareness;
- Analyzing the effectiveness of relevant security policies, regulations and requirements, leveraging data from the Regulatory unit.

[20] National Institute of Standards and Technology's Cybersecurity Framework: https://www.nist.gov/cyberframework

Good practice:
European Network and Information Security Agency (ENISA)

ENISA[21] works closely with countries in the European Union and with the private sector to deliver advice and solutions on cybersecurity. Their work includes:

- Activities that support policy making and implementation, such as recommendations on baselines security practices;
- Coordination of CERT cooperation and capacity building;
- Studies on emerging technologies;
- Analysis of the cyber-threat landscape.

Regulatory unit

The Regulatory unit should be responsible for the oversight and compliance with cybersecurity requirements established by legislation. As its primary tasks, it should:

- Create the necessary documentation and guidance so that organizations understand their obligations under all relevant legislation and can fulfill those obligations and interact appropriately with the regulators who will be enforcing these laws;
- Establish a process with clear points of contact, structure, and templates for organizations to report incidents, including clear timelines;
- Create and implement compliance and enforcement capabilities, if mandated by legislation;
- Manage engagement with sectoral regulators on cybersecurity domestically, in coordination with the Outreach and partnership unit;
- Measure progress using quantitative and qualitative metrics and work with policy and planning staff to assess effectiveness of the requirements on a periodic basis;
- Collaborate with the Policy and planning unit to develop and update regulatory obligations for security baselines, incident reporting, and drive alignment on various national and international regulatory requirements[22].

[21] https://www.enisa.europa.eu/
[22] https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

Microsoft
Building an effective
national cybersecurity agency

Good practice:
Germany Federal Office for Information Security (BSI)

The Federal Office for Information Security is Germany's federal regulatory authority, which shapes information security regulations for government, industry and the public. BSI conducts a range of activities to implement cybersecurity regulations, including:

- Developing criteria, procedures and tools to test and evaluate the security of information technology systems;
- Testing and evaluating the security of information technology systems and compliance with existing IT security standards, and issue security certificates as needed;
- Providing technical guidelines and procurement requirements for federal bodies;
- Analyzing information on security risks and providing the results to the relevant authorities;
- Providing support for law enforcement and other government authorities to carry out their legally mandated tasks;
- Producing key data, operating cryptography and security management systems for federal information security.
- International coordination on cybersecurity;
- Authorization of electronic signatures and cryptography services.

Collaboration with the Policy and planning unit will be important, especially on security baselines and incident reporting. Fundamentally, the two functions of policy and regulation are related but should be separated, with the former responsible for the development of the regulatory policy and the latter responsible for the operational implementation, in order to ensure a system of checks and balances. Furthermore, while both functions involve technical expertise, the expertise needed is different. Setting regulatory policy requires an understanding of the technology, risks, and security outcomes that need to be achieved. Oversight and enforcement of regulation is a more programmatic function involving collection, examination, review of documentation, and development and implementation of enforcement actions.

As such the Regulatory unit should be active in collecting documents, receiving reports, managing compliance, of the entities under its authority. In addition, this unit should also investigate whether an automated system of incident reporting might be possible, including an ability for organizations to amend and update incident reports, should new information become available. Such a development would be of fundamental utility for a Regulatory unit in light of the steady increase in the frequency and complexity of cyber-incidents.

Outreach and partnership unit

The Outreach and partnership unit should lead and manage relationships and interfaces across the government, institutions, the private sector and with other nations. The Outreach and partnership unit should create and manage intra- and inter-governmental advisory councils and public-private partnerships (PPP) to enable collaboration. Any effective focus on cybersecurity requires regular interaction, cooperation, and collaboration with industry partners to manage today's highly dynamic landscape of cyber risks. These councils and PPPs should advise the rest of the national cybersecurity agency on technologies, innovations, and risks. Specifically, it should address how these factors may affect the security and economy of the country, and effectiveness of current cybersecurity policies and regulations.

More broadly the unit should:

- Create intra-governmental advisory councils composed of cybersecurity representatives from across the government to facilitate dialogue and alignment of regulatory requirements;
- Coordinate and support engagement with domestic sectoral regulations on cybersecurity, in coordination with the Regulatory unit;
- Create and manage domestic public-private partnerships and promote PPPs composed of representatives from academia, industry and associations to advance and address specific security outcomes and challenges, and to inform the development and alignment of regulatory requirements;
- Serve as the point of contact for non-regulatory engagement on cybersecurity with the private sector;
- Engage and represent the government in the use of international PPPs, such as the European Cyber Security Organization (ECSO);[23]
- Coordinate and support relationships and engagements with other cybersecurity agencies internationally;
- Advance the formulation of national cybersecurity education plans, workforce development and awareness, such as participation in Cybersecurity Awareness Month;[24]
- Create and support outreach programs that extend nationwide and provide information to aid and empower small and mid-size enterprises (SMEs) and consumers on cybersecurity;
- Promote temporary industry exchange programs designed to train government officials with the newest technologies from the private sector.[25]

[23] European Cyber Security Organization: https://www.ecs-org.eu/cppp
[24] National Cyber Security Awareness Month: https://staysafeonline.org/
[25] https://www.ncsc.nl/english/Cooperation

Microsoft
Building an effective
national cybersecurity agency

Good Practice:
National Cybersecurity Center (NCSC) of the Netherlands

> NCSC recognizes that sharing knowledge is critical to cybersecurity and that it needs to be a two-way process, based on equality and trust. It therefore focuses on working with: various government parties; public and private parties; professionals in practice, education and academia; and international partners.
>
> In addition to individual partnerships, a networked approach has been developed and National Response Network (NRN) and National Detection Network (NDN) were launched to encourage greater dissemination of information.

Communication unit

The Communication unit should coordinate regulatory and non-regulatory communication, including messages, documents, publications, and statements to all stakeholders on behalf of the national cybersecurity agency. It should serve as the lead for communication during a crisis or emergency, and the primary point of contact for media, organizations and the general public seeking information about the agency's programs, policies, procedures, statistics, and services.

The Communication unit is critical to the ability of the agency to interact effectively with a wide variety of stakeholders, including the general public, industry partners, other governments and other CERTs. Effective communication is an essential component of responding to cyber-incidents. Microsoft believes that communication is the cornerstone for managing and mitigating damage in a crisis. As such, its role will be critical in ensuring that sensitive information is handled appropriately, that trust in partnerships is maintained, that all parts of the agency and other partners are effectively coordinating with each other to manage the situation, and that public confidence is maintained.

To be effective, the Communication unit should therefore:

- Manage public facing communication, including the agency's website and other traditional and social platforms;
- Develop communication in support of government-to-government and regulatory coordination;
- Disseminate technical communication in support of the work of the national CERT;
- Develop a crisis communication plan to ensure that in the event of an incident the government and other stakeholders are well prepared to communicate and thereby retain public confidence. The plan should include:
  - Clear points of contact within the cybersecurity agency;
  - Delineated roles and relationships between different organizations' communication functions when a cyber-attack occurs on government networks; and
  - Established policies on information sharing with the broader public on cybersecurity issues.

Operations unit / Computer Emergency Response Team (CERT)

The Operations unit should be tasked with ensuring effective coordination and deployment in response to cyber-threats. In effect, they should perform the work of a national CERT. There are numerous recommendations and good practices on structuring CERTs readily available, including those from the Forum for Incident Response Team (FIRST)[26] and Global Forum for Cyber Expertise (GFCE).[27] From these good practices, the recommendations for the Operations unit are:

- Work to facilitate voluntary sharing of information between the private sector and the CERT;
- Develop greater technical and operational capabilities for incident analysis and response;
- Ensure native malware analysis capabilities or have access to them on a contractual basis.

[26] FIRST: http://www.first.org/
[27] Global Forum on Cyber Expertise (GFCE): CSIRT Maturity Initiative: http://www.thegfce.com/initiatives

Microsoft
Building an effective
national cybersecurity agency

It is essential, however, to emphasize that for voluntary information sharing initiatives to be effective, a CERT needs to be clearly separated from the Regulatory unit. Private sector entities are often reluctant to share information with a public sector organization if the latter also has regulatory powers, for fear that the information might be used against them. The Operations unit and/or CERT should be exclusively focused on handling computer security incidents, and this separation of roles will be all the more important in the early days of the national cybersecurity agency, when relationships of trust are still being established.[28]

Malaysia Computer Emergency Response Team (MyCERT)

Operating from the office of CyberSecurity Malaysia, the Malaysian national cybersecurity agency MyCERT provides a point of reference for the Internet community in Malaysia on how to deal with computer security incidents. MyCERT provides assistance in handling incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security related incidents, as well as operates the country's malware research center.

MyCERT works closely with law enforcement agencies such as the Royal Malaysian Police, Securities Commission, and Bank Negara Malaysia. MyCERT also collaborates with Internet Service Providers (ISPs), computer security incident response teams and various computer security initiatives worldwide.

[28] https://www.mycert.org.my/en/index.html

5 Expect to evolve and adapt

Regardless of what the eventual structure of the national cybersecurity agency is, the unavoidability of change will require it to evolve and adapt over time, if it is to continue to fulfill its mandate. The drivers of change that seem clear even today are:

- Continuous and rapid evolution of ICT, and the related development of new tools and services;
- Increasing ubiquity of ICT within all aspects of human life and endeavor, as new tools and services are taken up by citizens, businesses and bureaucracies, and as the basic infrastructure of the Internet penetrates every corner of the globe;
- Ongoing exploitation of ICT for ends that are (potentially or actually) harmful or outright destructive to citizens, businesses and bureaucracies, whether by cybercriminals, intelligence organizations or militaries;
- Creation of new regional and international standards and baselines around cybersecurity, from risk management through to resilience;
- Possible emergence of wholly new categories of technology that fundamentally reshape the world as we currently know it, e.g. artificial intelligence.

For any national cybersecurity agency such developments could require the modification of the mandate, the acquisition of staff with new skills, fresh partnerships with public and private sectors or international organizations, and so on. In such a dynamic and evolving environment, it is critical that a national cybersecurity agency is able to make the necessary adjustments to its structure and operations, and has the authority to be listened to by policy-makers or legislators when requesting that those changes be made.

During the inception of a national cybersecurity agency, we therefore recommend the establishment of a regular processes to review agency performance and the nature of the changes taking place in the wider "cyber-world". Emerging good practices and newly established standards or baselines should be studied and most importantly, both the agency's private sector and civil society partners should be involved in the discussions, not merely of past performance but of future requirements.

Conclusion

We hope that this paper contributes to governments' thinking about establishing or restructuring their cybersecurity governance and that it proves a useful reference point. As the challenges and opportunities related to the proliferation of ICT continue to grow and evolve, governments will need to equip themselves accordingly. The creation of a strong national cybersecurity agency should be one of the options governments look at seriously.

It is already clear that as technology seeps into all aspects of our lives, the range of policy issues it affects, and that it is affected by, will multiply. This unusually broad scope cuts across traditional governance structures and government departments. It even takes policy-making out of the purely government sphere and into a more collaborative and partnership-oriented landscape than governments may be comfortable with. It will require policy-makers to work hand-in-hand with key national stakeholders from industry and civil society, rather than developing their approaches unilaterally. And it will require some level of policy cooperation across borders, not just with immediate neighbors but regionally and internationally.

For any government looking to develop a sustainable model of national cybersecurity governance, two things will be essential. First, that there is a process for engaging policy-makers with the aforementioned internal and external stakeholders who want effective and balanced cybersecurity policies. Second, that the governance structure has the capacity to evolve in light of developments in technology, society, and business.

A strong national cybersecurity agency can help governments manage all the different aspects of cybersecurity governance. Drawing on the five recommendations made in this paper, it can engage (within government itself, across the broader domestic context, and with other jurisdictions) and it can keep up to date with developments and adapt accordingly. Given clear ownership and power across the various functional areas it is expected to oversee, and equipped with the necessary capabilities and resources, a national cybersecurity agency can deliver not only for those who make the policy but also for those who take the policy, be they critical infrastructure providers, businesses, public sector organizations or even other regulators.


Microsoft