CYBER STRATEGY & POLICY BRIEF

STEFANOMELE
DIRITTO DELLE TECNOLOGIE - PRIVACY - SICUREZZA E INTELLIGENCE

Volume 10 – October 2016

EXECUTIVE SUMMARY

Keywords: *Association of South-East Asian Nations (ASEAN), Critical Infrastructures, Cyber Crime, Financial Sector, G7, National Security, Risk Analysis, Singapore, Strategy, Turkey, United States.*

In the middle of October, the Ministers of Finance and Governors of the Central Banks of G7 countries released the document entitled "*G7 Fundamental Elements of Cybersecurity for the Financial Sector*".

The purpose of the general principles outlined in this guideline is to provide a framework to develop cyber security strategies for those working in the financial field, both public and private.

The document easily and clearly combines the fundamental principles typical of every corporate risk management – either in finance or in other sectors.
The approach, in fact, could not be different, especially considering the variety of the financial companies such guidelines are addressed to, not only looking at the wide range of activities carried out but taking also into account their presence on the territory.

As regards actions taken in this field by some countries, Singapore and Turkey have released an update to their cyber security strategies.

It is undeniable that the Singaporean Government has been taking – and still takes – many actions in cyber security since 2013 up to date. Most of them, anyway, still seem to be too focused on the country itself or at most on ASEAN countries (Association of South-East Asian Nations).

To this end, in fact, it would be desirable that the Singapore Government showed to be more open to the other international players, so as to share experiences, information and best practices to counter cyber threats.
This is especially true for a country like Singapore which – as also stated in its new cyber security strategy – commits to be "*a secure and trusted hub*" at the international level in the field of cyber security.

The Turkish *National Cyber Security Strategy 2016-2019* is an extremely interesting document. Nevertheless, a clearer explanation, description and design of its strategic goals would allow for a more immediate comprehension and implementation of the strategy.

Beyond that, some actions the Turkish Government commits to take are highly remarkable – tough quite late, perhaps. They include the intention to create a national critical infrastructure inventory highlighting cyber security requirements and needs for each infrastructure, or to provide legal, and financial support and qualified personnel aimed to reinforce the *Cyber Incidents Response Team* (CIRT), as well as the intention to establish a central public authority responding directly to the Prime Minister to coordinate all governmental efforts in this sector.

An alphabetic list follows of the main cyber security related news and events of the last months about strategy and policies.

FOCUS ON THE DOCUMET "G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR"

In the middle of October, the Ministers of Finance and Governors of the Central Banks of G7 countries released the document entitled "*G7 Fundamental Elements of Cybersecurity for the Financial Sector*".

The purpose of the general principles outlined in this guideline is to provide a framework to develop cyber security strategies for those working in the financial field, both public and private.

This document indeed follows the provisions of the "*G7 Principles and Actions on Cyber*", a document issued at the end of May 2016 by the leaders of the G7 countries, and analyzed in detail in May 2016 *Cyber Strategy & Policy Brief*.

The "*G7 Fundamental Elements of Cybersecurity for the Financial Sector*" outlines eight general principles addressed to financial stakeholders, namely:

1. **Cybersecurity Strategy and Framework.**

   The scope is to establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.

2. **Governance.**

   The scope is to create effective governance structures to reinforce accountability by articulating clear responsibilities and lines of reporting and escalation.

3. **Risk and Control Assessment.**

   The scope is to evaluate the inherent cyber risk presented by the people, processes, technology, and underlying data that support each identified function, activity, product, and service.

4. **Monitoring.**

   The scope is to establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

5. **Response.**

   The scope is to timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed.

6. **Recovery.**

   The scope is to resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

7. **Information Sharing.**

   The scope is to engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning.

8. **Continuous Learning.**

   The scope is to review the cybersecurity strategy and framework regularly and when events warrant to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

As can be easy to infer, the document easily and clearly combines the fundamental principles typical of every corporate risk management – either in finance or in other sectors.

The approach, in fact, could not be different, especially considering the variety of the financial companies such guidelines are addressed to, not only looking at the wide range of activities carried out but taking also into account their presence on the territory.

What is surely remarkable, in fact, is the strong will of G7 Countries to focus their efforts also on problems related to cybersecurity – as already happened last May and as we can expect for the future, during Italy's next year presidency of the G7.

SINGAPORE

At the beginning of October, the Government of Singapore updated its cyber security strategy, by releasing a detailed and well-structured document, whose purpose is to outline the new medium and long-term development strategies in this sector.

Actually, since 2005 cyber security has been a key element of Singapore national policy. During the years, in fact, three strategies have been published. The first two, both known as *Infocomm Security Masterplan,* aimed at developing capabilities and expertise useful to safeguard the Public Administration information systems (2005) and critical infrastructures (2008) from cyber threats. The last one, made public in 2013 and known as *National Cyber Security Masterplan 2018*, is intended to protect the whole Government ecosystem, including businesses and individuals.

This last strategy has indeed been the starting point for the creation – in 2015 – of two key structures in the national organizational framework to counter such threats: the *Cyber Security Agency of Singapore* and the *Cybercrime Command*. The first one, within the Office of the Prime Minister, aims to centralize and coordinate all cyber security related agencies and initiatives already operative (i.e. *Singapore Infocomm Technology Security Authority* and *Singapore Computer Emergency Response Team*). The second one, instead, responds to the Ministry of Home Affairs, with the purpose to create an *elite* unit of *Singapore Police Force* specifically dedicated to national and international digital investigation.

The new cyber security strategic document, called *Singapore's Cybersecurity Strategy*, is based on four strategic and very broad pillars, but clearly focused on the most important and shared international requirements, namely:

1. **Building a resilient infrastructure.**

   The purpose is to safeguard primarily national critical infrastructures and their capability to supplying essential services to citizens. This can be done not only by raising the cyber security level of such infrastructures resorting to the well-known principle of "*Security-by-Design*", but also by developing well-structured and fine-tuned risk management processes and response and recovery plans.

2. **Creating a safer cyberspace.**

   The purpose is to continue countering cyber crimes both at home and abroad in a more and more coordinated and effective way, also protecting citizens' personal data. To this end, the *National Cybercrime Action Plan,* launched by the Ministry of Home Affairs in July 2016, shall play a definitely crucial role, once entered into force. Such *National Plan*, in fact, is based on four highly effective and practical strategic pillars, namely, preventing cyber crimes, constantly conducting horizon scanning of the criminal scenario and its evolutions, creating a robust and simplified criminal justice system, countering cyber crime as a national and international shared responsibility.

3. **Developing a vibrant cyber security ecosystem.**

   The purpose is to reach cooperation agreements with the private sector and academia to develop a cyber security culture, finally leading to a national ecosystem made of enterprises, start-ups, R&D programs in this field, as well as training qualified personnel.

4. **Strengthening International Partnerships.**

   The purpose is to develop strong cooperation and collaboration to counter international cyber threats and cyber crime, particularly with ASEAN countries (Association of South-East Asian nations).

As previously stressed, the analysis of *Singapore's Cybersecurity Strategy* shows an approach based on few pillars but with a broad scope. Nonetheless, the document appears to be coherent and well-focused on the main shared strategic priorities in the field of cyber security, as outlined by the main international players.

In addition, the long-term goals seem to be duly challenging for the protection and resilience of national critical infrastructures and especially contrast to cyber crime – this latter being closely linked to the *National Cybercrime Action Plan* entering into force.

It is undeniable that the Singaporean Government has been taking – and still takes – many actions in cyber security since 2013 up to date. Most of them, anyway, still seem to be too focused on the country itself or at most on ASEAN countries (Association of South-East Asian Nations).

To this end, in fact, it would be desirable that the Singapore Government showed to be more open to the other international players, so as to share experiences, information and best practices to counter cyber threats.
This is especially true for a country like Singapore which – as also stated in its new cyber security strategy – commits to be "*a secure and trusted hub*" at the international level in the field of cyber security.

TURKEY

Released at the beginning of September, but made public in English only in October, Turkey *National Cyber Security Strategy 2016-2019* updates the previous document entitled *National Cyber Security Strategy and 2013-2014 Action Plan*, providing new cyber security strategic guidelines for the period 2016-2019.

Turkey's previous strategy outlined 7 general guidelines to be implemented through 29 operational actions, accurately detailed in *2013-2014 Action Plan* and regarding both contents, and timing and people in charge of their implementation.

Interestingly enough, despite not actually implementing the entire *2013-2014 Action Plan*, the Turkish Government has in any case launched some remarkable initiatives during the years. This is in fact the case with *Ulusal Siber Olaylara Müdahale Merkezi* (National Cyber Incident Response Center) and its *Siber Olaylara Mildahale Ekipleri* (Team for Responding to Cyber Incidents), whose purpose is to provide constant and continuous assistance in identifying and countering cyber threats against Turkish national security. Not less remarkable are also the various actions for the protection of national critical infrastructures' cyber security taken by the *Türkiye Bilimsel ve Teknolojik Araştırma Kurumu* (Scientific and Technological Research Council of Turkey), or the creation, in 2012, of the *TSK Siber Savunma Komutanlığı* (Military Cyber Security Command).

The main two goals Ankara Government intends to reach thanks to the new *National Cyber Security Strategy 2016-2019*, are, instead, as follows: the first one aims at implementing any action necessary to make it clear for all the stakeholders that cyber security is an integral part of Turkish national security; the second one is targeted to spread ICT and governance competences needed for the public and private sector to reach and keep high cyber security levels.

The Turkish Government has identified 5 strategic pillars in order to achieve such goals, namely:

1. **Strengthening the Cyber Defence and Protection of Critical Infrastructures.**

   The purpose is to reduce risks deriving from cyber attacks, liable to affect Turkish economy, critical infrastructures and citizens.

2. **Combating Cyber Crimes.**

   The purpose is to reduce risks caused by criminal activities in and through the cyberspace that might affect Public Agencies and citizens.

3. Improvement of Awareness and Human Resources.

The purpose is to implement any action necessary to bring cyber security culture to all social classes and levels.

4. Developing a Cyber Security Ecosystem.

The purpose is to adopt, thanks to the help of all public, private and non-governmental stakeholders, any possible action to identify and implement all the legal requirements and technologies needed to develop a national cyber security ecosystem.

5. Integration of Cyber Security to the National Security.

The purpose is to take any action useful for all stakeholders to understand cyber security is an integral part of Turkish National security.

Yet, the *National Cyber Security Strategy 2016-2019* seems to be less stringent than the previous document in identifying timings and roles. In fact, although 18 operational actions have been outlined for the implementation of the 5 above-mentioned strategic goals, no reference is made – at least in the public version – to timings and respective responsibilities for actually implementing each of the guidelines above.

In addition to this, some actions the Turkish Government commits to take are highly remarkable – tough quite late, perhaps. They include the intention to create a national critical infrastructure inventory highlighting cyber security requirements and needs for each infrastructure, or to provide legal, and financial support and qualified personnel aimed to reinforce the *Cyber Incidents Response Team* (CIRT), as well as the intention to establish a central public authority responding directly to the Prime Minister to coordinate all governmental efforts in this sector.

To conclude, the *National Cyber Security Strategy 2016-2019* is definitely an extremely interesting document. Nevertheless, a clearer explanation, description and design of its strategic goals would allow for a more immediate comprehension and implementation of the strategy.

Notwithstanding, the document focuses of the main shared strategic priorities in the field of cyber security as identified by the main international players.

Finally, we need to point out that up to date the Turkish Government has attracted most of the critics for the difficulties found in coordinating a coherent and effective response to cyber attacks – despite the constant commitment of the *National Cyber Council*. To this end, it seems clear that, working under the Ministry of Transport, Maritime Affairs and Communications slows down its activities in case of cyber crises and especially limits its capability to have political and operational influence.

Such difficulties, though, might soon find a solution thanks to the new strategy. The commitment to establish a central public authority responding to the Prime Minister and aimed at coordinating all governmental efforts in the field of cyber security must in fact be one of the most relevant and urgent priorities while implementing the *National Cyber Security Strategy 2016-2019*.

UNITED STATES

The myriad of companies supporting the U.S. Government have always been one of the weakest links in an attempt to implement an effective defense and contrast strategy against cyber threats and especially cyber espionage.

Creating working solutions in the field of information security, by making such stakeholders aware and especially responsible for this, is extremely desirable for any Government that really wishes to safeguard their confidential information from cyber attacks carried out in and through the cyberspace.

This is the purpose of the *Final Rule* of the *Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities*, come into effect last November 3rd.

According to this rule, in fact, all contractors and their subcontractors carrying out any activity whatsoever for the U.S. Department of Defense must report within 72 hours any type of cyber incident occurred to their information systems.

Two fundamental principles are made clear in this rule: first, all companies in some way cooperating with the U.S. Defense must mandatorily share information on any cyber incident whatsoever occurred, then contractors must report any such information in the shortest time possible.

The purpose is clear, though unexpressed explicitly: not only to gather information on cyber incidents to safeguard ongoing development projects or programs, but also and especially to process it by using this information immediately in order to counter cyber crime, as well as for counterintelligence and national security activities.

In this regard, the *Final Rule* is extremely precise and explicitly stresses such goals, indicating as classified information to be shared any information useful for the U.S. Department of Defense for legal investigations of cyber incidents.

Such approach has in fact its grounds in the mandatory requirement for all contractors to share even "simple" breaches of internal security procedures.

This clarification is clearly aimed at limiting cases of classified information exfiltrated by any unfaithful employees – a particularly critical topic for the U.S., especially after what happened with Edward Snowden and, more recently, with Harold Thomas Martin III.

Thanks to the approach used, this information sharing program definitely differs from the much more renowned *Cybersecurity Information Sharing Act* (CISA), where information is collected and processed for the only purpose of information security.

The Final Rule entering into force shows once again the great effort made by the U.S. Department of Defense in the field of cyber security, seemingly having the most coherent and global approach to this sector.

ABOUT THE AUTHOR

Stefano Mele is an attorney specialized in ICT Law, Privacy, Information Security and Intelligence and works as '*of Counsel*' at Carnelutti Law Firm, Milan. He holds a PhD from the University of Foggia and cooperates with the Department of Legal Informatics at the Faculty of Law of the University of Milan. Stefano is also the Founding Member and Partner of the Moire Consulting Group and he is also the President of the "*Cyber Security Working Group*" of the American Chamber of Commerce in Italy (AMCHAM). He is Director of the "*InfoWarfare and Emerging Technologies*" Observatory of the Italian Institute of Strategic Studies 'Niccolò Machiavelli' and member of the International Institute for Strategic Studies (IISS). Stefano is also a lecturer for several universities and military research institutions of the NATO and the Italian Ministry of Defence and has published a number of scientific works and articles about cyber security, cyber intelligence, cyber terrorism and cyber warfare.
In 2014, his name appeared in the list of NATO *Key Opinion Leaders for Cyberspace Security*.
In 2014, the business magazine Forbes listed Stefano as one of the world's best *20 Cyber Policy Experts* to follow online.

For more information: www.stefanomele.it

SEE ALSO THE PREVIOUS VOLUMES

[…]

Cyber Strategy & Policy Brief (Volume 04 – April 2016)

Keywords: *Australia, China, Cyber Intelligence, Cyber Warfare, Germany, Information Dominance, Russia, Strategy, United States, U.S. Air Force.*

Cyber Strategy & Policy Brief (Volume 05 – May 2016)

Keywords: *Active Cyber Defence, Cyber Intelligence, Cyber Warfare, G7, Iran, Japan, Strategy, Supreme Council of Cyberspace, United Nations, United States, U.S. Naval Academy.*

Cyber Strategy & Policy Brief (Volume 06 – June 2016)

Keywords: *Cyber Command, Cyber Intelligence, Cyber Warfare, Israel, Israel Defense Forces, Italian Joint Command for Cyberspace Operations, Italian Joint C4 Command, Italy, NATO, Strategy, Ukraine, Ukraine National Cybersecurity Coordination Centre.*

Cyber Strategy & Policy Brief (Volume 07/08 – July/August 2016)

Keywords: *Cyber Warfare, Rules of Engagement for Cyberspace, FBI, DHS, ODNI, United States.*

Cyber Strategy & Policy Brief (Volume 09 – September 2016)

Keywords: *Cyber Warfare, Department of Homeland Security (DHS), Elections, Electronic Voting Systems, Espionage, Influence Activities, Information Warfare, International Law, Offensive Cyberspace Operations, Office of the Director of National Intelligence (ODNI), Propaganda, Russia, United Nations, United States.*