The global uptake of the NIST Cybersecurity Framework

The US National Institute of Standards and Technology ('NIST') Cybersecurity Framework ('Framework') is a voluntary, risk-based cyber security standard that was developed by consensus among thousands of participants from government, academia and industry. While the Framework's immediate purpose was to improve security and resilience in the US, its development was mindful of global needs for more standardisation in vocabulary and policies. Since its release, the Framework has drawn growing interest internationally, making it a valuable guide for all organisations to consider, both in the US and globally. Evan D. Wolff, Maida Oringher Lerner, Peter B. Miller, Matthew B. Welling and Christopher Hoff of Crowell & Moring describe here the Framework's uses and development, and discuss why it has proven attractive to organisations both in the US and elsewhere, and why this popularity continues almost two years after its original release.

President Obama's Executive Order 13,636: Improving Critical Infrastructure Cybersecurity called for the development of a voluntary, risk-based Cybersecurity Framework, essentially a set of standards, guidelines and practices that could help organisations manage their cyber risks[1]. In response, NIST[2] convened a year-long public-private collaborative effort, bringing together individuals and organisations from industry, academia and government, and released the Framework for Improving Critical Infrastructure Cybersecurity on 12 February 2014[3].

The Framework represents a public-private collaborative effort

The Framework represents a consensus description on what a comprehensive cyber security programme should include, providing organisations of all sizes and with varying levels of cyber security sophistication a guide for applying risk management principles and best practices. The Framework allows a variety of organisations to determine their current level of cyber security, set goals that are in sync with their business and establish a plan for both maintaining and improving their level of security. It also offers a methodology to help organisations incorporate privacy and civil liberty protections into their cyber security programme.

The Framework consists of three main elements: the core, tiers and profiles. The core consists of five functions: identify, protect, detect, respond and recover. Together, these functions allow any organisation to understand and shape its cyber security programme. The tiers describe the degree to which an organisation's cyber security risk management meets the goals set out in the Framework (i.e. from informal, reactive responses to an agile and risk-informed organisation). The profiles are intended to help organisations progress from their current level of sophistication toward targeted improvement.

The Framework establishes a common baseline that may be tailored to accommodate diverse stakeholders

When it was released, the Framework was important because it established a platform from which stakeholders could engage in collaborative efforts to identify and understand common issues, and work together toward common solutions. It also served as a general baseline for cyber security across critical but dissimilar industry sectors. The Framework provided a common starting point.

Since its release, the Framework continues to be useful as a baseline standard of care, particularly for organisations whose cyber security programmes are subject to US regulatory oversight. For example, the US Securities and Exchange Commission ('SEC') explicitly referenced the Framework in its cyber security guidance for the firms it reviews[4]. Also the Framework has been referenced in guidance from a variety of regulators and industry groups, including the US Department of Energy[5], the Financial Industry Regulatory Authority ('FINRA')[6], the US Food and Drug Administration ('FDA')[7], the US Federal Communications Commission ('FCC')[8], the Securities Industry and Financial Markets Association ('SIFMA')[9] and the State of Texas[10]. Use of the Framework to meet regulatory compliance obligations has also been underscored in enforcement proceedings initiated by the US Federal Trade Commission ('FTC')[11]. Most recently, the Obama Administration's Cybersecurity National Action Plan ('CNAP') references the Framework as an important building block for developing cyber standards to enhance US critical infrastructure security and resilience[12].

The Framework is intended to keep pace with a changing landscape

The Framework has always been intended to be a 'living' document that could be updated to keep pace with a rapidly changing landscape. Technology, threats and other factors are regularly changing, and the Framework was intended to be updated to incorporate evolving intelligence and lessons learned through its use. With the Framework, NIST also released an accompanying 'Roadmap' document that laid out a path toward future framework versions with this need for update in mind[13].

However, since the Framework was released, the landscape has continued to evolve, while the Framework has not. No updates have been released since the Framework's initial version, but developments have continued elsewhere. For example:

- The North American Electric Reliability Corporation ('NERC') is implementing Version 5 of its critical infrastructure protection cyber security standards ('CIP Version 5'), which becomes effective on 1 April 2016[14]. Because NERC is the regulatory authority that oversees the reliability of the bulk power system in the US, as well as parts of Canada and Mexico, CIP Version 5 is the cyber security standard adopted by the US power sector.
- The US Department of Defense ('DoD') continues development of the Safeguarding of Unclassified Controlled Technical Information clause (the 'Safeguarding Clause') of the Defense Federal Acquisition Regulation Supplement ('DFARS')[15]. The Safeguarding Clause applies to all DoD-funded contracts and establishes requirements for the handling of unclassified but controlled technical information by contractors. The Safeguarding Clause was initially finalised in November 2013, but an interim rule expanding its application was issued in August 2015[16].
- In June 2015, NIST released an updated Guide to Industrial Control Systems ('ICS') Security[17], which includes new and expanded guidance on how organisations should tailor traditional information technology controls to accommodate the unique performance, reliability and safety requirements of ICS. The new version of the ICS guide also includes updates on threats and vulnerabilities, risk management, recommended practices, security architectures and security capabilities and tools for ICS.

Additionally, and as contemplated with the Framework's release, the threat landscape continues to evolve. The prominent cyber breaches at Sony Pictures in 2014 and the US Office of Personnel Management ('OPM') in 2015, as well as the thousands of less publicised incidents, underscore this reality. As threats keep moving and changing, organisations and industries must also continue to adapt; they cannot rely - and are not relying - on one increasingly dated framework alone.

The Framework should evolve going forward

Despite the evolution of cyber threats and development of more stringent regulatory programmes, organisations are not casting the Framework aside. More typically, many organisations are using the Framework both as a starting point for evaluating their security needs and in concert with other standards of care in developing and deploying their cyber security programmes. The Framework also continues to serve as a common baseline for efforts across industries and in working with lawmakers, regulators and law enforcement in response to incidents that arise and when developing new policies.

As new legislation is enacted and regulatory policies continue to evolve, we expect that the Framework will continue to be a valuable tool for companies to use in meeting their compliance obligations. We also believe it will continue to be one particularly useful component for organisations to use as they develop their cyber security programmes, though its application may be in more of a backdrop function as more targeted programmes continue to be developed within industry sectors. To remain current, the Framework will also require regular updates.

Applying the Framework outside of the US

From the outset of the Framework's development, many companies expressed concern about the growing diversity of cyber security requirements throughout the world. The Framework was never intended to be a 'US only' guide as stakeholders were mindful of the need for greater global alignment of standards to avoid confusion, duplication of effort or even conflicting expectations[18].

Following the Framework's release, multinational organisations have been working to raise awareness and understanding outside of the US. For example, Microsoft has engaged Korea and Japan through a public-private delegation as well as additional outreach in Europe, Africa and the Middle East[19]. Such efforts are driven by companies' strong desire to avoid the costly - perhaps unworkable - task of doing business and developing products and services in a global environment with hundreds of varying national requirements[20]. Instead, these stakeholders are pushing for greater collaboration and coordination among government to harmonise their efforts.

Even without specific national adoption, the Framework is a useful guide for organisations globally

NIST has also been active in additional international outreach. For example, NIST was hosted by the European Commission for a November 2014 workshop to compare the Framework to development efforts underway for the European Union's Network and Information Security ('NIS') Directive[21]. NIST has also met with representatives from at least 20 additional nations[22].

With these efforts, awareness and acceptance are growing. Italy has incorporated the Framework into its National Framework for Cyber Security[23]. In January 2015, the UK announced that it would be working with the US to align cyber security best practices and standards between them, including explicit reference to the Framework[24]. Australia is expected to look to the Framework as it develops a national policy[25], and the chairman of the board of the International Organization of Securities Commissions ('IOSCO') has referenced the Framework as a successful starting point for cyber risk management[26]. As these examples demonstrate, global attention on the Framework is steadily growing.

There are lessons to be learned from the international privacy frameworks built for commercial data flows. The globalisation of privacy and cyber security is a necessity given the international nature of modern trade and data flows. The collaboration between the Asia-Pacific Economic Cooperation ('APEC') and European Union Data Protection Authorities with regard to international data privacy frameworks is an example of effective bridge building and public-private cooperation. APEC, which accounts for approximately 54% of the world's total GDP and 44% of the world's trade[27], developed through a global private-public collaboration (with 21 member economies involved) the Cross Border Privacy Rules ('CBPR') system and Privacy Recognition for Processors ('PRP'). The intention was to set a global standard for data privacy programmes[28]. Thus far, the United States, Mexico, Japan and Canada have joined the CBPR system, and all APEC member economies have committed to joining. Because the APEC systems were built with global trade and data flows in mind, they take cues from the globally recognised privacy principles upon which most privacy frameworks and privacy laws are built, including the EU system of Binding Corporate Rules ('BCRs'). APEC and the EU data protection authorities have even mapped their two systems and continue to work with each other to make global compliance easier for companies and cooperation easier for regulators.

Frameworks like the US-EU Safe Harbor ('Safe Harbor'), a principles-based programme which gave companies a voluntary but enforceable avenue to legally transfer personal data from the EU to the US, run into major hurdles when they do not change quickly enough to meet evolving threats and legal pressure. Safe Harbor was invalidated by the European Court of Justice in October 2015[29], and companies were left scrambling for alternative data transfer mechanisms. Safe Harbor collapsed under court order based on a perception that Safe Harbor was not enough to protect EU personal data. The intention all along was for Safe Harbor to evolve as needed to ensure continued protection and data flows, but the Safe Harbor framework documents were not updated over the 15 years of its operation. Luckily, the European Commission and the United States announced the successful renegotiation of Safe Harbor's replacement, the 'EU-US Privacy Shield,' in February 2016; and the programme is expected to be formally adopted and implemented within three months. The lesson to be learned is that government agencies that create these privacy and cyber security frameworks need to keep a careful watch over evolving patterns in trade, data flows, cyber threats, and political realities. Government agencies must then evolve with the times and cooperate with each other to provide framework updates in a timely manner and solutions that will bridge international divides. The EU and US have agreed to evolve more regularly in the future by committing to jointly review the EU-US Privacy Shield on an annual basis and update the framework as necessary based on these reviews[30].

Even without specific national adoption, the Framework is a useful guide for organisations globally. Most prominently, its guidance was developed through consensus among numerous cyber security experts and practitioners from government, academia and a variety of industry sectors, and it reflects their collective knowledge base. The Framework is also attractive because it was developed as a voluntary standard and can be deployed without adding regulatory requirements. In addition, the Framework is useful as a baseline standard of care that can be deployed across industries (and borders) and is logical and comprehensive, while also being a comparatively simple and cost-effective tool for organisations to address cyber risk based on their business needs.

Evan D. Wolff Partner

Maida Oringher Lerner Senior Counsel
Peter B. Miller Senior Counsel
Matthew B. Welling Associate
Christopher Hoff Associate
Crowell & Moring, Washington DC
ewolff@crowell.com

[1] Exec. Order No. 13,636, 3 C.F.R. § 13,636 (2014) available at https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] NIST is a non-regulatory federal agency within the US Department of Commerce. See General Information, NIST http://www.nist.gov/public_affairs/general_information.cfm

[3] NIST, Framework for Improving Critical Infrastructure Cybersecurity (2014) available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf; see also NIST Press Release, NIST, Releases Cybersecurity Framework Version 1.0 (12 Feb 2014) available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

[4] US SEC, Investment Management: Guidance Update, No. 2015-02 (Apr 2015) available at http://www.sec.gov/investment/im-guidance-2015-02.pdf

[5] US Dept. of Energy, Energy Sector Cybersecurity Framework Implementation Guidance (Jan. 2015) available at http://energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance

[6] FINRA, Report on Cybersecurity Practices (Feb 2015) available at http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

[7] US FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[8] US FCC, Communications Security, Reliability and Interoperability Council IV, Cybersecurity Risk Management and Best Practices Working Group 4: Final Report (Mar 2015) available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

[9] SIFMA, Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Business (July 2014) available at http://www.sifma.org/newsroom/2014/sifma_statement_on_the_nist_cybersecurity_framework/

[10] Texas Dept. of Info. Resources, Agency Security Plan available at http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=5

[11] See, e.g. FTC v. Wyndham Worldwide Corp., et al., No. 14-3514 (3d Cir. 24 Aug 2015). The Wyndham defendants settled with the FTC on 9 December 2015. See FTC, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk (9 Dec 2015) available at https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment

[12] See White House Press Release, Fact Sheet: Cybersecurity National Action Plan (9 Feb 2016) available at https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[13] NIST, NIST Roadmap for Improving Critical Infrastructure Cybersecurity (12 Feb 2014) available at http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf. NIST recently issued a Request for Information ('RFI'), seeking input from stakeholders about "the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance of the Framework." Request for Information, NIST: Views on the Framework for Improving Critical Infrastructure Cybersecurity, 80 Fed. Reg. 76,934 (11 Dec 2015).

[14] See NERC, CIP V5 Transition Program, http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

[15] US Dept. of Def., Def. Fed. Acquisition Reg. Supp., 252.204-7000 (Aug. 2013), http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

[16] Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), 80 Fed. Reg. 51,739 (26 Aug 2015).

[17] NIST, Guide to Industrial Control Sys. (ICS) Security, NIST Special Pub. 800-82 (2015) available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[18] NIST, Cybersecurity Framework FAQs: Relationship Between The Framework and Other Approaches and Initiatives at 43, https://www2.nist.gov/cyberframework/cybersecurity-framework-faqs-relationship-between-the-framework-and-other-approaches-and-initiatives#aligned

[19] In the Matter of Experience with the Framework for Improving Critical Infrastructure Cybersecurity, Response of Microsoft Corp. to Request for Info., RFI Docket No. 140721609-4609-01 (US Dept of Commerce 10 Oct 2014), available at http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf

[20] See, e.g., Jan Neutze, Positive Steps on the Road Towards Harmonization of Global Cybersecurity Risk Management Frameworks, Microsoft Cyber Trust Blog (19 Dec 2014), http://blogs.microsoft.com/cybertrust/2014/12/19/nis-platform/

[21] The European Commission, Parliament, and Council came to an agreement on NIS in December 2015, and after formal approval the NIS Directive will be implemented by all EU Member States. See European Commission Press Release, Commission Welcomes Agreement to Make EU Online Environment More Secure (8 Dec 2015) available at http://europa.eu/rapid/press-release_IP-15-6270_en.htm

[22] NIST, Newsletter Updated on the Cybersecurity Framework (1 July 2015), http://www.nist.gov/cyberframework/upload/csf-july2015-newsletter.pdf

[23] CIS-Sapienza and Laboratorio Nazionale Di Cyber Security, Framework Nazionale Per Law Cyber Security (2015) available at http://www.cybersecurityframework.it/

[24] Cabinet Office, Dept. for Bus., Innovation & Skills, Foreign & Commonw. Office and Nat'l Security and Intell., 2010 to 2014 Government Policy: Cyber Security (8 May 2015) available at https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

[25] See, e.g. Roger Parker, Developing an Australian Cybersecurity Framework, Australian Bus. Rev. (8 Sept 2015), http://www.businessspectator.com.au/article/2015/9/18/technology/developing-australian-cybersecurity-framework (discussing expected influence of the Framework).

[26] See, e.g. Sam Fleming, Market Watchdog Warns on Danger of Cyber Attack, Fin. Times (24 Aug 2014), http://www.ft.com/intl/cms/s/0/82519604-2b8f-11e4-a03c-00144feabdc0.html (discussing Mr. Medcraft's comments on American risk-management principles).

[27] Office of the US Trade Rep., US-APEC Trade Facts, https://ustr.gov/trade-agreements/other-initiatives/asia-pacific-economic-cooperation-apec/us-apec-trade-facts#

[28] Cross Border Privacy Rules System, http://www.cbprs.org/

[29] European Court of Justice Press Release, The Court of Justice Declares That the Commission's US Safe Harbour Decision is Invalid (6 Oct 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[30] European Commission Press Release, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (2 Feb 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm