Discussion Draft of the NIST Cybersecurity Framework (CSF) 2.0 Core

NCC Group's response, May 2023

Introduction

NCC Group is pleased to offer its observations in response to the National Institute of Standards and Technology's (NIST) discussion paper.

We support NIST's objectives to develop practical performance-oriented guidance for critical infrastructure operators and other organizations as they look to secure their supply chains from fast-evolving third-party supplier risks. In doing so, we strongly believe that NIST's approach to supply chain risk management – particularly the requirements outlined under sections GV.RM and ID.SC in the draft CSF – could be further strengthened and future-proofed by **taking a more holistic view of risk and adopting more explicitly a 'Resilience by Design' approach**.

While we note that the CSF's focus is on cybersecurity, related non-technical risks such as supplier failure, service deterioration, and concentration risk often overlap with – or in some cases are caused by – cyber risks. We therefore believe that supply chain risk management should be considered in the round and ask that NIST – perhaps through the Software and Supply Chain Assurance Forum – consider how a holistic approach might be implemented. As global experts in risk management, NCC Group would be happy to present our case to the Forum, if that would be of interest.

Taking a holistic approach to managing supplier risks

We are in favour of a broader definition of supply chain resilience that looks beyond technical cyber risk and takes a wider approach to understanding what is needed to safeguard continuity of service and operational continuity against non-technical risks such as insolvency, administration and liquidation, transfer of ownership, service deterioration, and concentration risk. We have sought to introduce to regulators' considerations of operational resilience the concept of **'Resilience by Design'**, assuming supplier failure by default, and taking a two-fold approach to mitigating the associated risks that include:

- **prevention of supply chain failure** (through cyber resilience solutions); and,
- **mitigation of the risk and impact of supply chain failure** (through technology and software/data escrow agreements).

In that context, we welcome existing NIST guidance – including NISTIR 8276 - that details practical considerations for organizations managing their cyber supply chain risk. In particular, we note the acknowledgement of the role escrow services can play as part of a formal C-SCRM program. However, we strongly believe that such services not only have a core role to play in mitigating cyber risk associated with suppliers who have "a questionable or risky track record" – as noted in the guidance - but should form part of the temporary stages of business continuity and stressed exit plans for all business-critical applications as part of a holistic risk management approach. **While we recognise the CSF's focus on cybersecurity, we do also believe that wider third-party risks should be considered and reflected in NIST's updated CSF.**

In practice, this should include naming supplier failure, service deterioration and concentration risk as risks that require mitigation strategies (e.g. through stressed exit plans and scenario testing), and

assigning ownership for third-party risk at the highest-possible level. Indeed, this holistic approach has been adopted across several regulators globally, including the Prudential Regulatory Authority (PRA) in the UK[1], the European Union[2] and the Monetary Authority of Singapore[3].

Role of cloud, software and technology escrow agreements

We would emphasize the difficulties in exhaustively identifying a suppliers' risk profile, given it is generally the result of a combination of a multitude of factors. Identifying all possible scenarios is likely disproportionate to its potential benefits, and would likely lead to increasing costs and creating barriers to innovation. For that reason, we do believe that cloud, software and technology escrow solutions can offer legal, technical and proportional assurance to critical infrastructure in dealing with their third-party suppliers, particularly where they embrace the concept of 'Resilience by Design'. This would **assume supplier failure by default, regardless of their risk profile, and encourage or mandate using cloud, software and technology escrow agreements as a proportionate and cost-effective solution for regulated entities to mitigate against this**. Indeed, escrow agreements and verification services act as a technical insurance policy and business continuity strategy, safeguarding the long-term availability of business-critical technologies and applications while protecting intellectual property.

Establishing cloud, software and technology escrow agreements with supporting verification services will create a baseline to:

- Grant organizations access to the source code and the right to access the cloud environment where it is hosted, where: an application is material to the organization's operational continuity, if the service is deployed in the cloud; or if the application presents a concentration risk. Indeed, the role of escrow agreements is reflected in CISA's guidance on ransomware[4] which states that, in being prepared for a ransomware incident, organizations should ensure the availability of source code through backups or escrow agreements. The details of any access rights and conditions will be set out in individual agreements, offering a legal basis with full transparency for all involved parties over when any such rights can be invoked.

- Specify how the agreement and access rights are to be used in the event of supplier compromise / failure. This goes beyond cyber risk, taking a broader view which includes non-technical risks such as bankruptcy / liquidation / insolvency, failure to maintain / inability to fix the service, transfer of ownership of intellectual property rights to the software, or the supplier organisation as a whole, unless the new owners agree to keep in place the agreement. Principally, critical infrastructure rely on failed services continuing to operate while full recovery plans are being implemented. That means that continuity and exit planning needs to take account of implementation, testing and training times that impact on the ability to exchange or replace products and services expediently, safely and compliantly.

- Advance capabilities to automate risk tolerance at the application programable interface (API) gateways level to permit control to gracefully failsafe services or providers who may go out of compliance, removing exposure latency in a real-time digital economy.

[1] SS2/21 'Outsourcing and third party risk management' (bankofengland.co.uk)
[2] Digital finance: Council adopts Digital Operational Resilience Act - Consilium (europa.eu)
[3] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
[4] Ransomware Guide | CISA

Many critical infrastructure organizations – particularly those in the financial services sector – already use escrow solutions as part of their comprehensive business continuity planning when mitigating supplier risk, and some third-party service providers themselves have opted to build these solutions into their offer to support their customers' compliance with regulatory requirements.

By way of example, NCC Group has worked with a banking technology provider on developing a cloud escrow solution. The provider's cloud hosted digital banking software-as-a-service (SaaS) solutions supports more than 6,000 loan and deposit products serving over 14 million end customers worldwide. Working with NCC Group, the provider adopted a cloud escrow solution to establish a robust approach to its customers' regulatory compliance, offering business continuity assurance by ensuring that financial institutions deploying the provider's solution would have access to their application and specific cloud environment as well as support for the ongoing maintenance and management of their application.

However, we believe that there is still insufficiently widespread awareness of the benefits of software and technology escrow solutions, and the role they can play in addressing regulatory requirements on outsourcing and third-party risk management. To address this lack of awareness, **we believe that there is a role for NIST – working with sectoral agencies and global counterparts – to do more to promote and educate organizations on the benefits of cloud, software and technology escrow solutions** as a practical means to meet outsourcing and risk management requirements. This could be through explicitly encouraging the mandating of escrow solutions or by encouraging much greater inclusion of it in implementation guidance. This would align with approaches taken by other regulators, particularly those in the financial services sector as outlined above, as well as CISA's aforementioned guidance on ransomware.

Conclusion

NCC Group welcomes the opportunity to contribute to NIST's discussion paper. We have positively contributed to other regulatory authorities' consideration of cybersecurity, operational resilience and third-party risk management. As noted above, we would welcome the opportunity to engage in more proactive dialogue with NIST to support its objectives. NCC Group is able to offer interactive dialogue with its IT technical experts, solutions architects and qualified legal advisers each of which have years of experience in navigating the mitigation of risks for clients.

About NCC Group

With **over 30 years' experience protecting business critical software, data and information through escrow, secure verification testing, and cloud hosted software continuity services,** as well as significant experience securing digital transformation programs, increasing resilience and reducing risk. NCC Group has followed regulatory developments regarding supply chain risks and third-party arrangements closely, not least to ensure that we, too, are able to meet our customers' evolving demands as regulatory requirements change. We work with customers operating across critical infrastructure sectors who understand how cybersecurity and software resilience can add value and represent a competitive advantage both in their own business as well as across their portfolios. We hold a unique position where we see compliance from the end-user's perspective as well as from the viewpoint of the IT provider, and try to assist both in achieving their aims.

NCC Group is a global cybersecurity business headquartered in the UK. Through its $220m acquisition of Iron Mountain's Intellectual Property Management division (IPM), has an **established**

and significant footprint in North America, alongside our existing presence in Europe, the Middle East and Asia Pacific. This means we are able to take an international perspective to regulatory approaches to cybersecurity and third-party risk management. The IPM business has been operating in the North America regulatory market for over 30 years. We believe strongly in the potential of appropriate regulatory measures to unleash the innovative ingenuity of adjacent services sectors to develop practical solutions that allow organizations to meet regulatory requirements in the most effective way.