Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

NCC Group's response to NIST's request for information, April 2022

Introduction

NCC Group is delighted to offer its observations in response to the National Institute of Standards and Technology's (NIST) request for information.

We fully support NIST's objectives to align its Cybersecurity Framework with the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) and develop practical performance-oriented guidance for critical infrastructure operators as they look to secure their supply chains from fast-evolving third-party supplier risks. In doing so, we believe it will be critical to **establish common criteria supporting periodic assessment** and **ensure that the roles and responsibilities of managing supply chain security are established and understood** from the outset. In addition, we strongly believe that NIST's approach to supply chain risk management could be further strengthened and future-proofed by **taking a more holistic view of risk and adopting more explicitly a 'Resilience by Design' approach**.

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, but, 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.

The scale and complexity of the challenge

Supply chain compromises are symptomatic of a lack of investment to pay down technical debt: "fixing supply chain security" will not be done quickly or easily.

NCC Group's latest research shows that supply chain attacks were one of the top three types of cyberattack to increase in the last 6 months, behind phishing and malware and attacks of operational technology. Concerningly, our survey of approximately 1,400 cyber-security decision makers at large companies[1] found that only one in three (32%) respondents were "very confident" that they could respond quickly and effectively to a supply chain attack. Despite this gap between the rate of attacks and organizations' ability to deal with them, just one in four (24%) named third-party and supplier risk as a major cybersecurity challenge for the next six to 12 months. Many plan to invest in new third-party software, hardware and SaaS security products in 2022, which could further complicate organizations' supply chains and increase their attack surfaces.

Getting every organization to the same level is, in our view, not practical and highly unlikely to be achieved (and should not be the objective in any case). Organizations struggle to understand what good supplier cybersecurity would look like; are uncertain regarding the best approach to wider supply chain monitoring (e.g suppliers' suppliers); make assumptions that larger suppliers will adhere to stringent cybersecurity standards; report a disconnect between procurement and IT security teams; are worried about the burden on smaller suppliers as well as worried about the lack of choice or dominance of some suppliers who can dictate terms due to their market power.

Articulating outcomes

The "importance of supply chain security" can often be a nebulous concept that becomes difficult to define, and even harder to measure and evaluate. To address this, we believe NIST should articulate the desired outcomes of NIICS clearly. We would argue that these outcomes might be different for different stakeholders – from nation state, to industry sector, company and individual citizen – and that these differentiated outcomes should be communicated transparently.

We propose the following as a starting point for further discussion, arguing that security improvements across the digital supply chain should measurably:

a. **Reduce the risk of low-level suppliers being used as entry points for far-reaching cyber intrusions and attacks in a quantifiable manner by 2025**;

b. **Reduce the risk of suppliers falling victim to a cyberattack that disrupts their service delivery, with significant knock-on effects for their customer ecosystem**;

c. **Mitigate the impact of supplier disruption or failure more broadly.** It is worth highlighting that we argue 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/failure to maintain services, 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 take 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). As we outline in more detail below, we would suggest the building of stressed exit plans and the testing of these plans to ensure viability. Indeed, this approach has been adopted across several financial

[1] Supply chain security risks are providing a back door for hackers | NCC Group Newsroom

regulators globally, including the Prudential Regulatory Authority (PRA) in the UK[2] and the Monetary Authority of Singapore[3].

Clarity of accountability

Clarity is needed over who will be held accountable for which outcomes. Our survey[4] found that there is significant confusion among organizations about whether a company or its suppliers are responsible for keeping them secure. Around one in three (36%) of respondents said that they are more responsible for preventing, detecting and resolving supply chain attacks than their suppliers, whilst just over half (53%) said that their company and its suppliers are equally responsible for the security of supply chains.

Supply chain security is a beautiful but largely abstract concept. We need to break down what we think it means in terms of who has to do what for whom, for what purpose and how will it be measured. **While we would argue, at a high level, that supply chain security should be a core part of corporate governance, and similarly adhere to the principle of "ownership = responsibility", we equally propose asking, and answering, very practical questions that go to the heart of how supplier assurance might be achieved in reality**, such as:

a. Is it the buyer's responsibility to demand security assurances from their suppliers?

b. Is it the supplier's responsibility to offer security assurances?

c. Is it the manufacturer's responsibility to take care of products that suppliers buy and ultimately use in their services offered to other organizations?

d. Where does the responsibility of one part of the chain start, and end?

Embedding a 'Resilience by Design' approach

We are passionate in our advocacy for a greater regulatory-driven focus on the adoption of cloud, software and technology escrow solutions as the baseline implementation of what we're calling 'Resilience by Design', to meet critical infrastructure's increased demand for third-party risk management, business continuity and operational resilience.

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 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. 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 risks increasing costs and creating barriers to innovation.

---

[2] SS2/21 'Outsourcing and third party risk management' (bankofengland.co.uk)
[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] Supply chain security risks are providing a back door for hackers | NCC Group Newsroom

For that reason, no less, 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 / compromise 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**, by offering a minimum level of resilience through the legal and technical means to ensure continuity of services while a service is being restored and/or alternative options are being implemented. In this sense, 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[5] 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 company 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.

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 banking technology provider Mambu on developing a cloud escrow solution. Built within Amazon Web Services (AWS) infrastructure, Mambu's cloud hosted digital banking software-as-a-service (SaaS) solutions supports more than 6000 loan and deposit products serving over 14 million end customers worldwide. Working with NCC Group, Mambu 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

[5] Ransomware Guide | CISA

Mambu'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 – to do more to promote and educate other regulatory authorities and critical infrastructure operators on the benefits of cloud, software and technology escrow solutions** as a practical means, and a baseline Resilience by Design solution, to meet outsourcing and risk management requirements - be that 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[6], as well as CISA's aforementioned guidance on ransomware.

Additional Resilience by Design elements could include:

- **Ensuring the development and regular testing requirements of business continuity and exit plans forms part of licensing or contractual agreements** between regulated entities and their third-party suppliers, particularly through the release lifecycle of critical applications.

- **Broadening business continuity and stressed exit plan requirements** so that:

    - Cloud providers should advise their software vendors initiate stressed exit plans where the latter provide services to critical infrastructure.

    - Software contained within other solutions, as well as the internal infrastructure of third parties supplying software and technology solutions, should also be subject to stressed exit plans.

- **Mandating interchangeability of services between cloud providers, and regular testing of the interchangeability.**

    - The need for interchangeability between cloud services is already widely acknowledged. It is, however, important that the long-term goal of achieving widespread interchangeability is clearly set out, or it will remain a problem.

    - We believe that the European Commission's proposed Data Act offers an interesting proposal in this regard. The Act includes proposals to mandate cloud computing portability obligation, with the intent to make it possible for organizations to switch between cloud computing service providers, or port data back to on-premises IT systems without contractual, technical or economic barriers, offering clarity on what the technical requirements and timeframes are for 'cloud switching', as preconditions for portability of infrastructure, platform and software cloud services.

    - We believe that cloud escrow solutions, much like those offered by NCC Group, would act as a practical supplier failure and cloud portability solution, enabling contractual and technical portability.

[6] For example, the Prudential Regulatory Authority (PRA) in the UK which considers escrow solutions as one of a number of relevant resiliency options for firms to consider when undertaking business continuity and exit planning: SS2/21 'Outsourcing and third party risk management' (bankofengland.co.uk).

In addition, **we advocate for greater information sharing to improve shared and contextualised understanding of concentration and cyber risk** through elements including:

- Anonymous outsourcing arrangement audits to gain early insights and intelligence on emerging dependencies and criticalities.

- Firms' assessments of non-material outsourcing arrangements from the outset so as to be able to track trends over time, for example, where non-material services are supplied by a single provider to a large number of critical infrastructure organizations.

- Failed business continuity and stressed exit plans, particularly where these plans relate to larger suppliers.

Conclusion

NCC Group very much welcomes the opportunity to contribute to NIST's call for information. We have positively contributed to other regulatory authorities' consideration of cybersecurity, operational resilience and third-party risk management and 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.