You Outsource the Service but Not the Risk:
Supply Chain Risk Management for the Cyber Security of Safety Critical Systems

Chris. W. Johnson DPhil, School of Computing Science, University of Glasgow, Glasgow, UK.

Keywords: Supply Chain Risk Management, Outsourcing, Safety Requirements, Cyber-Security.

Abstract

Companies increasingly form interdependent relationships between contractors and sub-contractors that extend across national borders and legal jurisdictions. In consequence, supply chain risk management (SCRM) is an increasing concern for the cyber security of safety-critical systems. The following pages argue that outsourcing undermines SCRM by eroding technical expertise, which companies need to select and audit their suppliers. They are still held accountable when the failure of a sub-contractor jeopardizes the continuity of critical national infrastructures. Subsequent sections present SCRM techniques that support the cyber-security of safety-critical applications and at the same time help to realize the benefits of vertical market integration. Rather than de-risking, the aim of the paper is to reiterate that 'safety-critical organizations outsource the service but they do not outsource the risk'.

Introduction

Outsourcing offers many benefits. Companies focus on their core business. Sub-contractors provide economies of scale and specialization by offering the same services across a large number of customer organizations. Outsourcing is often also associated with 'de-risking' when companies are unsure of the best technology to invest in. Rather than acquiring costly capital items they can transfer the risk to the sub-contracting organization that must then purchase and maintain infrastructure components (Ref. 1).

These benefits must be balanced against a number of concerns. Companies often fail to draft service level agreements that place appropriate contractual requirements on sub-contractors. Particular areas of concern include clauses that specify minimum response times following system or service failures. Even if contracts have been carefully drafted, sub-contractor fail to meet desired levels of service if they lacks necessary technical competence or they are let down by their own suppliers. The following pages use examples drawn from Air Traffic Management to illustrate these concerns because the industry is experiencing new levels of change as we move to the deployment of the European SESAR and North American NextGen programmes. For instance, the introduction of performance-based navigation involves the computation of 4D trajectories in time and space from the point of departure rather than the sector-by-sector coordination of individual aircraft. In the past, Air Navigation Service Providers in Europe and North America supplemented in-house engineering teams with a small number of suppliers. However, the safe optimization of next generation concepts involves close cooperation between many different sub-contractors, any one of whom can introduce cyber-vulnerabilities into this safety-critical system of systems.

Safety Concerns in SCRM

Concerns over out-sourcing affect many different industries. However, they are particularly important for critical infrastructure providers where suppliers have a profound impact on non-functional requirements, including safety and security. It is important that companies monitor the performance of their contracts, especially when suppliers are unfamiliar with the additional requirements that characterize safety-related industries and where compliance may not be sustained over time (Ref. 2, 3). This might seem obvious – however, many organizations use out-sourcing to justify internal redundancies. Over time this erodes their technical competence to determine whether or not sub-contractors are meeting their contractual obligations (Ref. 12).

Supply chain risk management (SCRM) helps determine appropriate levels of trust in the vertical integration of complex industries. Operations research accounts for the costs and benefits of outsourcing as well as the potential consequences from supply chain failures (Ref. 4). Mathematical modeling techniques have also mapped transitive networks of trust across a number of industries (Ref. 5). However, there has been little attention on the impact that SCRM has for the cyber-security of critical applications. Many safety-related industries face a growing range of

cyber threats and it is hard to identify vulnerabilities that are inherited from systems and processes that cross organizational boundaries.

Direct Supply Chain Risks: Direct supply-chain risks stem from the use of out-sourcing contracts for critical information services within a safety-critical organization. Distinctions can be made between Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Most often these refer to Cloud architectures but they have wider application in safety-critical infrastructures. Companies can use the IaaS model to outsource the provision of computation hardware. Sub-contractors acquire and maintain network infrastructures. This is typical of many existing agreements within Air Traffic Management, for example, where the maintenance and operation of Communication, Navigation and Surveillance support may be provided by external organizations. IaaS creates obvious concerns when contracting organizations have to trust the safety and security mechanisms of the IaaS providers. If outsourcing fails and critical hardware is unavailable then this will undermine continuity of service. It can also place employees and members of the public at increasing levels of risk. It is, therefore, critical that service level agreements do not simply focus on functional characteristics. They must also identify KPIs and audit mechanisms that identify safety and security concerns before an accident or incident occurs.

Platform as a service (PaaS) extends the hardware provision in IaaS to include development environments. PaaS concepts are often employed within safety-critical organizations but control is frequently retained within the company (Ref. 6). In other words, IT departments specify a baseline configuration across operational systems and this is then used to support a broad array of application programs (Ref. 7). There are some examples where Air Navigation Service Providers have used out-sourcing to implement PaaS architectures. One argument used to justify the delegation of computational infrastructure to external sub-contractors is the need to impose greater internal discipline on procurement decisions and to refactor legacy applications so that they will run in a common, enterprise architecture (Ref. 8).

Software as a service (Saas) extends PaaS; companies rent software from external organizations. This not only removes the need to maintain underlying hardware as in IaaS, or supporting operating/development environments as in PaaS, but also includes application software. The European SESAR Joint Undertaking has demonstrated increased levels of virtualization supporting radar and flight plan correlation, flight data distribution, flight data management, coordination and transfer through remotely-connected sites. The SESAR partners provide ANSPs with access to this new generation of virtualized software applications. Operational staff have little idea nor are they necessarily concerned to know where these infrastructure services are running. The level of implicit trust increases at each step from IaaS to PaaS to SaaS. Software as a Service often requires that organizations inform their operational and tactical decision-making using software that is owned and operated by external organizations.

Indirect Supply Chain Risk: SCRM is a transitive concept. Indirect risks threaten the computational infrastructures that support sub-contracting companies. They are ‘indirect’ because vulnerabilities are inherited from companies with which safety-critical organizations do not have any direct contractual relationship and hence may not be able to influence their operating practices or security measures. For example, Air Traffic controllers maintain separation by making sector-by-sector changes to aircraft routing. In contrast, the SESAR and NextGen programmes propose performance-based trajectories. Flight Management Systems calculate efficient routings in space and time, from departure to arrival. These are communicated to en route ANSPs across shared data networks and protocols. This depends upon interaction between dispatchers, airline operations centers, and meteorological agencies. These organizations, in turn, rely on third-party IT service providers across different countries. Such indirect interdependencies create significant concerns for SCRM. It is very hard to estimate the probability or consequences of knock-on service disruptions; either through ‘benign’ faults or malicious attacks. End-user organizations must develop extensive contingency plans to maintain safe and successful operation across highly distributed supply chains.

Downstream Supply Chain Risks: Companies must also account for the safety risks that they pass downstream to their customers. For example, problems in the supply chain might lead to the loss of Communication, Navigation or Surveillance functions for an ANSP. If they have adequate redundancy and diversity then backup systems can be used to limit the impact on airlines. However, safety concerns may eventually force the closure of airspace with a significant impact on the general public. Identifying appropriate levels of diversity and redundancy is not simply a technical concern. It is also determined by financial constraints. The economic necessities that motivate

outsourcing also erode the additional resources that be available to mitigate the downstream impact of supply chain failures (Ref. 2).

Cyber Security Concerns in SCRM

It is increasingly difficult to safeguard distributed, vertically integrated supply chains that extend across national borders. Many of the previous concerns are generic; they do not simply apply to cyber-security. In contrast, the following sections identify vulnerabilities and potential threats that threaten the supply chains that support many safety-critical industries.

The Loss of Security Through Obscurity: In many safety-related industries, attackers need motivation and opportunity combined with the technical knowledge that is necessary to conduct an attack. In the past, this would have been relatively difficult in domains such as Air Traffic Management; different ANSPs used a range of bespoke and specialist middleware. The last twenty years have seen a gradual drift towards mass-market software infrastructures based around Linux, GPS Augmentation Systems and Voice over IP. The introduction of these Commercial Off The Shelf (COTS) components creates the opportunities for companies to engage general sub-contractors who do not specialize in safety-critical applications. Previously, sub-contractors would have required specialist knowledge in the esoteric software that was only used within those technical domains. In contrast, the use of mass-market software provides more and more people with the technical background to perpetrate an attack. Related concerns stem from the exploitation of vulnerabilities in mass-market, office-based software to penetrate more secure, isolated operational systems during the Stuxnet and December 2015 Ukrainian attacks (Ref. 10). This has, typically, occurred when information is exchanged between the systems in order to generate reports to management of operational KPIs. These attack methods suggest that the same sub-contractors should not work on both operational and enterprise systems, in order to support SCRM.

Performance Based Regulation: Regulatory agencies used to focus on product based approaches to safety assessment. Standards specified the key attributes that products must possess in order to be considered acceptably safe, as typified by UK regulations based on the Factory Acts. This approach could not be applied to the logical abstractions in complex, software-based systems. It is impossible to identify a canonical set of properties that might be required over thousands of different software applications. There are significant technical barriers in verifying that particular properties hold across millions of lines of code, each relying on intermediate software and hardware to correctly implement the intended semantics of a higher level language. In consequence, process bases standards such as IEC 61508 and ED-153 have encouraged regulators to look more at the methods that are used in software development from planning through requirements to deployment and decommissioning. This approach has proven to be costly and also suffers from problems of independence when regulators almost become part of the development teams.

The UK Civil Aviation Authority is one of several regulators who are actively promoting performance-based regulation . This focuses on the measurement of KPI's. Previous incidents can be analyzed to identify potential precursors that raise safety or security concerns. Performance can be measured by the frequency of those precursors rather than a very low number of accidents. Regulators no longer need to be so closely involved in day-to-day development. This reduces the need for regulatory competency in a range of different software engineering practices. It also supports an 'arms length' approach to regulation, which in turn encourages the use of sub-contracting. Regulators focus on the KPIs, they do not need access to the development practices of external organizations who may be based in different member states. However, this development also raises new concerns. Not only do the contracting organizations outsource technical expertise to their suppliers. The regulatory agencies may also gradually suffer an erosion of technical competence if the focus on performance obscures detailed judgments about the methods used to meet those targets. This is a particular concern for the introduction of new technology into safety critical systems where regulators may not have sufficient insight to identify appropriate KPI's leading to regulatory lag – for instance over the introduction of Remotely Piloted Autonomous systems (drones) into controlled airspace.

The Insider Threat Across the Supply Chain: Outsourcing through diversified supply chains means that companies cannot always control who has physical or logical access to the infrastructures that they rely on. Many ANSPs now conduct background checks on their ATSEP engineers. However, this is seldom possible for all of the staff employed by a sub-contractor. These problems are exacerbated with a sub-contractor also relies on outsourcing, for

instance to supplement their own technical staff during periods of peak demand. IaaS, SaaS, PaaS architectures provide external staff with access that circumvents firewalls and intrusion detection systems that otherwise protect safety-critical systems. In many cases, external staff can enter company premises, attach their own devices and memory media to internal infrastructures and potentially expose critical systems to unprovenenced software.

Unprovenenced Software: Previous sections have argued that the increasing use of COTS infrastructure creates vulnerabilities in safety-related industries, including Air Traffic Management. More people have the technical competence to attack these systems. There is also a growing commercial market in zero day exploits. The rise of COTS is linked to outsourcing because it opens up services to a far wider range of sub-contracting companies than was ever possible for bespoke, specialist infrastructures. There are other concerns. In particular, SaaS and PaaS architectures can make it difficult for companies to monitor the code that is being integrated into the infrastructures that are provided by sub-contractors. In Air Traffic Management, the lack of regulatory guidance on cyber-security has led to a host of dangerous practices. Sub-contractors will still integrate unprovenanced code into critical applications – including libraries from public code repositories and Internet sources, not simply those that are provided with mass market compilers (Ref. 10). Previous sections have mentioned the ubiquitous use of Linux by ANSPs. There are numerous concerns over open-source collaborations in safety and security critical environments. It can be argued that code inspection by a committed community of developers increases the quality of the platform. It can also be argued that open source code exposes vulnerabilities to potential attackers and even creates the opportunity for the deliberate contribution of insecure code. These general arguments have taken on a particular twist within air traffic management where each sub-contractor has developed their own variant of Linux. Very few of these are POSIX compliant and their exact architecture is typically regarded as proprietary. This makes it incredibly difficult for ANSPs to access the technical information that is required in order to support SCRM.

Problems in Coding and Configuration Compliance: Cyber-security concerns increasingly impose additional coding and configuration standards on safety-related organizations, including baseline requirements in ISO27k. When companies retain control over internal software development, external procurement, through deployment to operation and maintenance then they can also retain a degree of control over these coding and configuration standards. This can be compromised through outsourcing, in particular with SaaS and IaaS, unless external contracts provide for audits to monitor compliance. Sub-contractors can offer better levels of service; many safety-critical organizations suffer from extremely low level of compliance with security requirements. However, the cost savings associated with outsourcing can make it hard for companies to retain sufficient staff with the technical expertise to determine whether or not sub-contractors are acceptably secure in their working practices (Ref. 9, 10).

Intellectual Property Barriers: Many safety-critical organizations focus narrowly on the financial savings that can be made through outsourcing. This is justified in conventional applications, the whole point of IaaS, PaaS and SaaS architectures is that the customer need not focus on the implementation mechanisms that are used to provide particular services. In other domains, this raises significant concerns for SCRM – you can outsource the service but you do not outsource the risk. This is particularly true in Air Traffic Management – where will be held accountable by politicians and the public even if the underlying cause of an incident stemmed from infrastructure that is under the control of a sub-contractor. The previous section has argued that companies must ensure they have sufficient competence to assess the sub-contractors ability to meet safety and security requirements. This raises particular concerns when external organizations might view such audit mechanisms as an infringement of their Intellectual Property Rights. There are ways of addressing these concerns – for instance, using government regulators to identify and monitor approved suppliers within an industry. Later sections will also argue for the use of safety and security cases to help document the technical interface between contracting company and sub-contractor. However, these solutions must be considered in the early stages of negotiation for contracts and service level agreements. They also, typically, imply additional costs that must be shared across the parties involved in these negotiations.

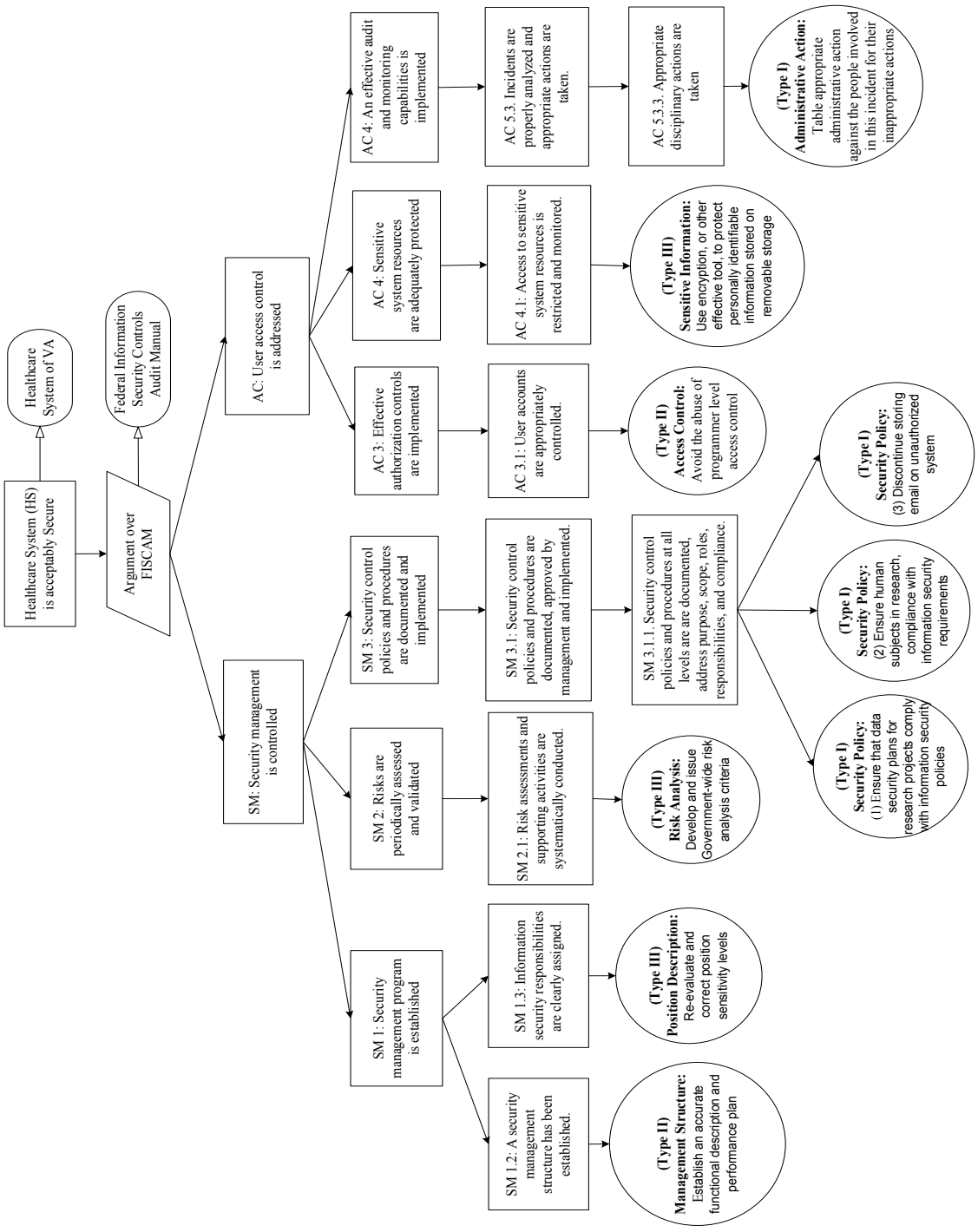
Improving SCRM for Safety and Cyber-Security

The previous paragraph sketched two potential approaches to Supply Chain Risk Management. The following sections identify further mitigations for the safety and cyber-security concerns that arise from outsourcing across critical infrastructures.

The Role of Security Cases: Safety cases model the arguments that explain why a system is acceptably safe. They have also been extended in a number of ways to represent the reasons why critical infrastructures are acceptably

secure. There are several different graphical notations that can be used to contrast these arguments. These offer many benefits for SCRM. For instance, Figure 1 shows how the leaf nodes in Goal Structure Notation (GSN) can be used to denote the evidence that is available to support claims about safety and security.

Figure 1 — GSN Illustrating a Security Case (Ref. 11)



These diagrams provide an overview of the output from hazard analysis as well as mitigation actions, including architectural designs and the results from validation or verification activities. Figure 1 focuses on evidence about

security practices within different departments of a single healthcare organization. However, the GSN can easily be extended to map out the arguments why an acceptable level of security can be achieved across organizational boundaries within a supply chain. The documents that provide evidence of security risk assessments and mitigation actions, denoted by the leaf nodes, can then be inspected to determine the quality of the evidence without necessarily compromising the IP barriers that protect commercial assets for sub-contracting organizations. Regulators can also use these graphical structures as maps to focus and direct audit activities.

Many questions remain about the use of safety cases in SCRM. For example, the documents represented as leaf nodes in a GSN are conventionally maintained by a single infrastructure organization. It seems clear that the rise of outsourcing will force the development of hybrid structures where some of the safety and security arguments are constructed and maintained by external partners. This creates problems of coordination and communication. In particular the UK Ministry of Defence Haddon Cave report argued that safety cases often become 'tick box exercises' unless evidence is challenged with the benefit of operational experience. For example, if evidence is obtained that undermines a safety or security argument then the GSN must be updated to reflect the new concerns. It is unclear how to ensure that this happens in a GSN that is distributed across a complex supply chain and where the sub-contractors may be at different levels of safety/security maturity.

Internal Diversity in the Supply Chain: Safety and Security cases provide an overall structure for arguments about SCRM. They must be supported by appropriate design and development techniques that can be used across distributed supply chains. These concerns can be illustrated by the use of diversity and redundancy in critical infrastructures. Conventionally, redundancy has been used to increase the reliability of safety critical systems. If a primary component fails then a backup is available. This approach cannot work in most software applications unless there is also an element of diversity. In other words, if one piece of code fails because of a bug then a redundant but identical piece of code will also fail in the same way given the same inputs because it will also have the same flaw. Techniques such as N-version programming have been used to counter this – two or more different companies supply redundant code because they are unlikely to suffer from the same bug. This assumes that the bug did not stem from a flaw in common requirements.

Unfortunately, the use of N-version outsourcing raises new complications when security concerns are considered. Although this approach provides strong technical support for safety requirements, it creates significant issues for cyber security. The diversity requirement implies that companies must now maintain and secure multiple supply chains. Insider attacks come stem from each one of the sub-contractors providing redundant code. Vulnerabilities might be propagated from configuration problems in any of their implementations. Some initial solutions have been proposed – for example, some ATM infrastructure companies will provide primary and secondary systems using different technologies. This offers diversity from a single supply chain – with benefits not only for security and SCRM but also for the administration of external contracts. Such approaches will only be successful if suppliers can avoid common mode failures across their diverse product lines – if primary and secondary systems contain similar failure modes then redundancy will be lost along with the trust of their customers.

Contract Transparency through Audit: Very few conference papers consider the importance of contractual relationships in safety or security critical systems. A key theme in previous paragraphs has been the need for companies to pay more attention to the terms under which they outsource key infrastructure services. In particular, contracts must consider the transitive relationships that arise when sub-contractors themselves rely on outsourcing. We would argue that the rise of service oriented architectures increases rather than diminished the need for technical competency within the end user organization. Unless companies know the questions to ask potential suppliers there is a significant risk that reduced costs will only come at the expense of reduced levels of safety and security. Contracts need to sustain and preserve intellectual property rights but at the same time enable customers to justify the trust that they place in their suppliers.

Monitoring and audit must ensure that contractual requirements for safety and security are met across extended supply chains. This not only applies to individual companies but also to government regulators. There is a danger that performance-based regulation undermine the technical competency that protects the public and encourages market development. It can be difficult to identify KPIs that reflect the safety and security not only of primary suppliers but also of sub-contractors across a supply chain. Very few tools or techniques have been developed to address these concerns. Caveat emptor (let the buyer beware).

Conclusions

Recent years have seen a growing reliance on mass-market software in safety-critical industries. These include but are not limited to Linux, VOIP communications and GPS augmentations systems based on EGNOS. One side effect has been a growing reliance on sub-contractors from other industries who may not understand the importance of safety and cyber-security requirements.

This paper has identified a range of concerns associated with outsourcing in critical infrastructures. The focus has been on understanding Supply Chain Risk Management (SCRM). The loss of security through obscurity, mentioned above, means that more and more attackers have the technical knowledge necessary to identify and potential exploit vulnerabilities across the supply chain. At the same time, the rise of performance based regulation based on KPIs rather than a detailed understanding of development processes, can undermine regulatory competence. KPIs are often only applied to first tier suppliers rather across their distributed supply chains. Other concerns stem from the insider threat when outsourcing provides more people with access to critical components and systems. External suppliers may also provide routes for unprovenanced software to be introduced into the supply chain. Intellectual and legal barriers can prevent companies from ensuring that coding/configuration standards are maintained.

We have also identified a number of potential solutions. These include high-level modeling such as the use of safety and security cases, where many different companies provide evidence of conformance across distributed supply chains. We have also summarized more detailed development architectures – in particular the nascent market in single-supplier diversity for the provision of redundancy in safety and security critical systems. We have also stress the need for improved contracts where levels of service are augmented with requirements for transparency and audit in order to maintain confidence across the supply chain. We have also argued that regulators require new tools and techniques that can be used across national and al borders. Until these are established, it is important to reiterate that while companies can outsource a service they cannot outsource the supply chain risk.

References

1. G. Elena and C.W. Johnson, Laypeoples' and Experts' Risk Perception of Cloud Computing Services, International Journal on Cloud Computing Services and Architecture, (5)4/5, August, 2015.

2. C. Vroom and R. Von Solms. Towards information security behavioural compliance. Computers & Security 23.3 (2004): 191-198.

3. O. Dahl. Safety compliance in a highly regulated environment: A case study of workers' knowledge of rules and procedures within the petroleum industry. Safety science 60 (2013): 185-195.

4. Wang, Jian-Jun, and De-Li Yang. "Using a hybrid multi-criteria decision aid method for information systems outsourcing." Computers & Operations Research 34.12 (2007): 3691-3700.

5. A. Durowoju, O., Kai Chan, H. and Wang, X., 2012. Entropy assessment of supply chain disruption. Journal of Manufacturing Technology Management, 23(8), pp.998-1014.

6. Diez, Oscar, and Andrés Silva. "Resilience of cloud computing in critical systems." Quality and Reliability Engineering International 30.3 (2014): 397-412.

7. Foster, Kevin D., et al. "Cloud computing for large-scale weapon systems." Granular Computing (GrC), 2010 IEEE International Conference on. IEEE, 2010.

8. C.W. Johnson, Identifying Common Problems in the Acquisition and Deployment of Large-Scale Software Projects in the US and UK Healthcare Systems, Safety Science, (49)5:735-745, 2011.

9. D. J. Bodeau, R. Graubart, and J. Fabius-Greene. Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) Levels. Social Computing (SocialCom), 2010 IEEE Second International Conference on. IEEE, 2010.

10. C.W. Johnson, Barriers to the Use of Intrusion Detection Systems in Safety-Critical Applications. In F. Koorneef and C. van Gulijk (eds.), SAFECOMP 2015, 375-384, Springer Verlag, Heidelberg, Germany, LNCS 9337, 2015.

11. Y. He and C.W. Johnson, Generic Security Cases for Information Systems Security in Healthcare. In Proceedings of the 7th IET Conference on Systems Safety and Cyber Security, Edinburgh, Scotland, 15-18 October 2012, IET, Savoy Place, London, 2012.

12. K. Langfield-Smith and D. Smith. Management control systems and trust in outsourcing relationships. Management accounting research 14.3 (2003): 281-307.

Biography

Chris Johnson, DPhil, School of Computing Science, University of Glasgow, Glasgow, Scotland, G12 8RZ, Scotland, U.K., telephone – +44 (141) 330-6053, facsimile – +44 (141) 330-4913, e-mail – Johnson@dcs.gla.ac.uk.

Chris Johnson is Professor and Head of Computing Science at the University of Glasgow in Scotland. He leads a research group devoted to improving the cyber-security of safety-critical systems. He has developed forensic guidance on behalf of the UK civil nuclear industry and helped develop European policy for the cyber-security of aviation – including ground based and airborne systems.