Centralised IT Structure and Cyber Risk Management

Kamran Abbasi[1], Nick Petford[2] and Amin Hosseinian-Far[3] [0000-0002-2534-9044]

[1,2,3] University of Northampton, Northampton NN1 5PH, UK
{[1]Kamran.Abbasi, [2]Nick.Petford, [3]Amin.Hosseinian-Far}@Northampton.ac.uk

Abstract. Against the backdrop of organisational needs to derive value from IT Organisations through agility, efficiencies and cost effectiveness, many organisations have adopted a decentralised IT organisational structure, enabling individual business units the autonomy to implement, operate and govern technology. The increase risk that poses organisations through cyber-attacks, raises the question of how IT security could effectively provide the level of organisations governance to counter cyber threats in a decentralised organisational model. In exploring the challenges in the decentralization of IT security, we highlighted that the accountability of such activities would become diluted, with each business unit managing security in their own methods and practices or lack of, while unable to take full accountability due to the complex independencies of modern system architectures, often resulting in a lack of ownership, accountability and reporting of security at an organisational group level. This ultimately increases the overall security risk to the organization. We further highlighted that while centralization of IT security at a group level would be more effective, a hybrid model of IT security at two-levels with strategy and policy at the central governance level and a degree of autonomy and decision at the IT Operational level could also be considered.

Keywords: IT, Information Security, Cybersecurity, Centralisation, Decentralisation, IT Organization, IT Value

1 Introduction

As businesses compete with one another for the competitive edge and dominant market share, it has become evident that IT can play a crucial role in enabling firms to meet their strategic objectives [1]. Firms may have to increase their investments in Information Technology (IT) to remain efficient, innovative, agile, and compete against their market competitors.

As Pajic et al. [2] highlight the increasing use of information technology has resulted in firms needing to evaluate the productivity impact of IT investments through IT value measures [2]. However, IT value has been a continuous discussion for organisations. Lei & Huifan suggest that organisations are challenged to determine the overall organisation performance generated by IT capabilities [3].

In today's organisations, data is considered as a treasured asset, which with appropriate data analytics techniques, can enhance business decision makings [4]. Lowry [5] argues that modern business organisations increasingly depend on their IT departments, he further goes on to suggest that IT Organisations are not merely expected to provide supporting services but more so becoming strategic partners and providing value-added services, moreover aligning its objectives and priorities with those of the departments and organisations overall strategy [5].

Lowry and Wilson's view relies on the assumption that IT performance will be optimised to meet the businesses demands and needs. Often IT performance is criticised for the lack of service quality and agility to meet the requirements of the broader organisation [5], as Whyte et al. suggest that IT organisation often failed to support businesses efficiently and in particular to change business attitudes and satisfy user needs [6].

This can result in organisations moving towards outsourcing their IT Services to third party organisations or decentralisation of the internal IT organisation and its capabilities. Moreover, it is against the backdrop of organisations move towards decentralisation of their IT capabilities and the increased risk of security breaches and the implications of them to an organisation's reputations and revenue that this paper aims to review some of the critical considerations of a Centralised IT security capability.

2 IT Security in IT Organisations

As the growth of online channels such as e-commerce and mobile commerce continues to increase and become a key revenue generator and strategic objective for most organisations, the need for robust IT Security governance has also become apparent. While previously IT security was often seen as a reactive measure, afterthought or over-head cost, the growing pressures to keep data and systems safe from customers, stakeholders and government regulators has forced organisations to elevate proactive and robust security measures [7], which includes people, technology and process considerations [8].

According to Hooper & Mckissack [9], in the past ten years, cybersecurity breaches have cost organisations worldwide billions of dollars. Most notably, technology firms such as eBay, Adobe Systems, AOL and Sony Interactive Entertainment's PlayStation Network have suffered heavy losses, resulting in widespread media reporting and served to attract organisation and public awareness of the potential damages of security breaches [9]. For this paper, security is defined as the protection against undesirable disclosure, destruction, or modification of data in a system and also the protection of systems themselves [10]. There are three key elements which underpin this definition, and these are vulnerabilities, exploits and threats.

- Vulnerabilities - these are bugs, weaknesses or flaws found in the design of the system architecture or processes which allow attackers to comprise these vulnerabilities to execute nefarious activities such as un-authorised access to data, Phishing or denial of service attacks (DDoS) [11],

- Exploits - these are actions which are executed by attackers on the identified vulnerabilities using various tools and techniques, often for purposes of self-satisfaction or financial gain [10] [11],
- Threats – these refer to the impending risk of an exploit that may be executed on identified vulnerabilities. Threats enable organisations to put in place countermeasures to mitigate and nullify the vulnerabilities and potential attack.

Whilst the importance of IT Security for an organisation is apparent [8] [9] [10], Organisations have in recent years been faced with the dilemma of centralising or decentralising their IT capabilities.

Brynjolfson, in his paper titled 'information assets, technology and organisation' [12] explained how information technology had the potential to significantly affect the structure of organisations. Almost 26 years on there remains a debate on how best to formulate the IT Organization within the context of the wider organisation. A continued 'merry-go-round' has witnessed the early popularity of centralisation to decentralisation in the 1980s and then re-centralisation of the 1990's [13]. In recent years with the growing disruptive digital phenomena and organisation drivers to promote innovation and agility [14], businesses are again seeking to ask the question whether to centralise or decentralise their IT organisations.

King [15] makes the basic assumption that centralised IT benefits the organisation by economies of scale while decentralised IT benefits by economies of scope [15]. Centralisation of IT versus decentralisation of IT refers predominantly to three key aspects. Firstly, the control of autonomy of decisions making in the organisation. Centralised organisations largely concentrate the decision into a single business unit, person or a group of individuals, while decentralisation primarily means devolving the decision-making authority and autonomy to individual departments and business units. This is supported by Richardson et al. [16] report from a 1987 study by Przestrzelski suggesting decentralisation can be broadly defined as "a dynamic, participative philosophy of organisational management that involves selective delegation of authority to the operational level" [16].

In the context of IT Security, individual business units would now have the freedom to make their own security-related decisions, such as the procurement and delivery of software, hardware, security governance and processes, controlled use of administrative privileges, and vulnerability assessment and remediation activities. Secondly, the physical location of resources. Centralisation often has resources in one place, while decentralisation spreads resources across multiple locations within the organisation. Thirdly, capabilities and functional activities. In centralisation, control and governance of functional capabilities would be driven from a central competency centre, while in decentralisation the functional capabilities would be disseminated across single or multiple business units.

In traditional organisations IT security has often fallen under the CIO organisation providing centralised security governance, and compliance, Hooper & Mckissack [9] argue that while this arrangement made sense, the downside resulted in IT security often being diluted in the plethora of other capabilities that IT was responsible for, not only in relation to priority but also budget allocation, with IT security often fading into the background unless there are had been a major security breach [9]. Whilst the authors do not advocate the decentralisation of IT security to individual business units within an organisation, they do however pose the question of where best fits a central IT security capability within an organisation. The authors highlight that while placing a central IT security function under the CIO could have benefits of synergies between both functions and efficiencies resulting in greater value for the organisation, this could also result in inhibitors for the security capability to highlight security threats, vulnerabilities and exploits of the CIO function. Whilst, separating the two functions out also comes with the challenge of diluted accountability as much of the security governance and principle are reliant on the underpinning IT systems and processes.

3 Centralisation and Decentrlisation of IT Security

For most organisation, the risk of IT security breaches remains high, ensuring business continuity, threat avoidance, quick incident resolution and disaster recovery. In a decentralised model, the accountability of such activities becomes diluted with each business unit managing security in their own methods and practises or lack of, while unable to take full accountability due to the complex independencies of modern system architectures, often resulting in a lack of ownership, accountability and reporting of security at an organisational group level. King [15] explores aspects of both centralising and decentralising. He suggests that centralisation of control preserves top management prerogatives, capitalising on economies of scale and to preserve organisational integrity in operations. The economies of scale arise from exploiting the full potential of technologies that cause the output to increase more rapidly than costs. The costs of duplicating overhead and facilities can be avoided, and organisational protocols are easier to enforce, while decentralisation allows lower-level managers discretion and authority in decision making, while also fostering a culture of innovation of new opportunities and responsibility for their decision making, possibly improving their performance. However, decentralisation of control may lead to problems of accountability and decision making if lower-level managers lack key competencies and are not held accountable for decisions [15]. King’s point on key competencies and accountability is particularly pertinent to IT Security. Khallaf & Majdalawieh examined whether the CIO's competency is a determinant of IT security performance measurement. The study highlights that CIOs' knowledge in IT acquired through their education or work experience improves the performance of IT security [17]. The study reaffirms King’s [15] viewpoint that by decentralising capabilities there may be a loss of key skills and competencies, with IT security itself being a complex domain which requires experience, knowledge with security architectures, processes and governance professionally designed [18]. To explore this view further, we explore some of the most common attacks cybersecurity vulnerabilities that organisations face today and how they would be complicated in a decentralised security landscape. Several studies have attempted to classify, characterise and provide recommendations to tackle cyber and cyber-enabled threats and security implications e.g. [19] [20]. A study by Humayun [10] Identified and analysed common cybersecurity vulnerabilities. The findings highlighted that Denial of service (DoS) was the most commonly addressed vulnerability (37%). The second most common vulnerability was Malware (21%), and finally, the third most common was Phishing (9%) [10]. We can see from the authors' research that all three vulnerabilities constituted to 67% of cybersecurity threats that organisations encounter today. In order to understand this better, we describe some of their key characteristics.

3.1 Malware

Malware is a shorthand term used for malicious software. In this attack, software programs are deployed on to user computers or servers to gain unauthorised access. The intent behind these types of attacks is to compromise organisational network devices in order to gain control of the host systems and networks for malicious aims [10]. A variety of malware types exists such as Viruses, Trojan Horses, Worms, Ransomware and Spyware. One of the most recent trends, Ransomware, a type of Malware has over the last five years gained prominence [21]. Ransomware is where a victim of an attack is blackmailed. According to Cartwright and Cartwright [21] there approximately hundreds, if not thousands, of ransomware strands in the wild [21].

Two such examples of Ransomware have been the cyber-attack that affected more than sixty NHS trusts in the United Kingdom, with 200,000 computers affected globally. The impact of this resulted in many facilities unable to access patient records which led to delays in surgeries and cancelled patient appointments [22]. The second of the attacks was that of South Korean web-hosting firm Nayana paying a $1 million ransom in 2017 clearly demonstrates how lucrative Ransomware can be for attackers [21].

3.2 Denial of Service (DOS)

Denial of service attacks have been around for many years, and they are triggered by a flood of network requests to an organisation's servers and networks, ultimately bringing the infrastructure down and enabling attackers to access vulnerabilities during the infrastructures recovery phase for bringing services back up. Large organisations have not been immune from DOS attacks, Yahoo, Amazon.com, eBay, CNN.com, Buy.com, ZDNet, were all subjected to total or regional outages of several hours caused by distributed denial-of-service (DDoS) attacks [23].

3.3 Phishing

Phishing is one of the most common forms of cyber-attack. Phishing works by attackers deceiving people with socially engineered approaches of downloading Malware or surrendering sensitive data such as passwords, personal information or bank details.

Curtis et al. [24] highlight that whilst technologies have evolved with organisations deploying tools such spam filters to effectively detect and deter known phishing campaigns, attackers continuously find new ways to evade these technologies such as through sophisticated and personalised e-mails ("spear-phishing") that take advantage of human limitations and biases and persuade people to respond [24].

Considering the impact that the previously described vulnerabilities can cause to organisations, rather than decentralise IT security processes, governance and capabilities, it is apparent that organisations should strategically align their IT Security and Business in way that it meets business needs, goals and strategies [25]. In the case of the NHS malware attack, it was identified that due to a lack of centralised security investment that many of the Windows operating systems were more than 15 years old and were no longer updated or supported by Microsoft [22].

Kearns and Lederer (2000) highlight the while IT Investment plans are often planned in isolation it is the utmost importance that IT and business investment plans are aligned on the strategic objectives of the organisation in order to obtain effectiveness (Kearns and Lederer, 2000). Furthermore, El Mekawy et al. [25] suggest that Information security processes (ISP) are an integrated part of IT strategy and business operations [25].

4 Information Security Processes

Centralised Information security can enable organisations to implement security risk-assessment processes. According to Laliberte [26], conducting risk-assessments are not only a good idea but can help organisations determine where organisations should invest their efforts both financially and effort to reduce its security exposure [26]. Laliberte [26] further argues that more importantly, risk assessments help to identify the key assets they need to protect and the threats and vulnerabilities those assets face. By assessing the likelihood of an incident and the effect of the incident actually occurring, the organisation can make a more informed decision about how and to what extent it should proceed to protect that asset. In essence, the risk assessment covers six key phases:

1. Asset identification;
2. Threat assessment;
3. Vulnerability assessment;
4. Risk determination;
5. Identification of countermeasures;
6. and finally, Remediation planning.

Oppliger [18]goes further to posit that the output of the security risk assessment goes further than just remediation planning, It forms the basis of the security policy, strategy and architecture at a technical, organisational and legal level [18].

Whilst Security risk assessments make sense, a study by Hooper & McKissack [9] found that the use of formal assurance techniques based on risk and security metrics at a central level did not always provide effective insights and communications tools to senior executives [9]. The survey resulted in these key findings:

- 75% of respondents indicated that metrics were important or very important to a risk-based security program.

- 53% didn't believe or were unsure whether the security metrics used in their organisations were properly aligned with business objectives.
- 51% per cent didn't believe or were unsure whether organisations metrics adequately conveyed the effectiveness of security risk management efforts to senior executives.

With these challenges already existing at a centralised IT security model, it would only be compounded by decentralising IT security in how to formulate, capture, measure, consolidate and action the overall security posture of an organisation, resulting in an increased risk of security breaches.

Lowry & Wilson [5] posits that centralised organisations that meet or exceed the service qualities of their business partners, the organisation, in turn, is far greater to derive IT related benefits. Conversely, if IT quality is low the organisation's ability to innovate and respond to market conditions will be hindered, leading the business to alternative IT models such as decentralisation. Magnusson [13] further support this notion from research on a case study of a large Swedish organisation, where he notes that a level of IT Support quality had resulted in some departments having to abdicate from IT altogether, decreasing their usage and even matters of organisation compliance [13]. While the literature supports that there is a relationship between IT perception of Service quality, there is a contradictory element, whereby although acknowledging the lack of IT service quality, some organisations may refrain from outwardly recommending decentralising. This may be down to a market context, whereby the concern of the available skills in less developed economies may act as an inhibitor to decentralise the IT organisation or that there is a lack of agreement on the key organisational objectives that drive the centralisation/decentralisation of IT

King [15] sets out organisational measurements/objectives of IT that drive the discussion on centralisation and decentralisation. This study adapts Kings models to incorporate Security aspects for an organisation:

- The need to provide IT security capability to all organisational units that legitimately require it.
- The need to contain the capital and operations costs in the provision of computing services within the organisation.
- The need to satisfy special computing needs of user departments
- The need to maintain organisational integrity in operations that are dependent on computing, i.e., avoid mismatches in operations among departments.
- The need to meet information requirements of management and security of the data.
- The need to provide computing services in a reliable, secure, professional, and technically competent manner.
- The need to allow organisational units sufficient autonomy in the conduct of their tasks to optimise creativity and performance at the unit level, while not putting the organisation at a risk of security breaches

- The need to preserve autonomy among organisational units, and if possible, to increase their importance and influence within the larger organisation, however, key capabilities with the required high level of governance such as IT Security remain centrally governed.
- The need, wherever possible, to make the work of employees enjoyable as well as productive.
- The need to counter security threats, vulnerabilities and exploits.

5 Conclusion

In summary, whilst a complete decentralising of IT Security capabilities across the organisation would create lack of governance, diluting accountability, increasing cost and skills while increasing the risk of IT security breaches there are rational arguments for both centralisation and decentralisation of the IT security function. Magnusson [13] highlights that centralisation and decentralisation may not be 'opposites or alternatives' but as mutually dependent. The model that Magnusson refers to the hybridisation of IT at two-levels with strategy and policy at the central governance level and a degree of autonomy and decision at the departmental/business unit level. This model also supports findings of Richardson et al. [16] that high performing organisations included those with simultaneous decentralisation and centralisation at two levels of the organisation [16]. Furthermore, in relation to IT Security, Hooper & Mckissack [9] support the notion of a hybrid configuration, with an introduction of a CISO (Chief Security officer) reporting to the CEO.

The configuration would be a split between operations and the more strategic level. For example, the IT department would be in charge of the day-to-day technical security operations while the CISO would operate independently and be responsible for the strategic aspects of the organisation's security posture. In conclusion, the impacts of IT security breaches for organisations are both vast in terms of financial and reputational damage. Organisations should keep consistency through centralisation of IT Security with two options 1) Complete centralisation of IT security at an IT level; or 2) a hybrid configuration with a CISO reporting to the CEO as a strategic security capacity and IT performing the day-to-day security operations underpinned by the Strategy of a CISO. Rather, Organisations should refrain from devolving IT Security responsibilities in a decentralised manner to individual business units which will only lead to dilution of responsibility, accountability of security capabilities and governance across the organisation increasing the risk of security breaches and attacks.

References

[1] A. Cane, "Information technology and competitive advantage: Lessons from the developed countries," *World Development,* vol. 20, no. 12, pp. 1721-1736, 1992.

[2] A. Pajić, O. Pantelić and B. Stanojević, “Representing IT performance management as metamodel,” *International Journal of Computers Communications & Control,* vol. 9, no. 6, pp. 758-767, 2014.

[3] C. Lei and W. Huifan, “Design and construct IT Performance architecture: settle the IT productivity paradox from critical realism,” *Procedia engineering,* vol. 174, pp. 537-542, 2017.

[4] J. Campbell, V. Chang and A. Hosseinian-Far, “Philosophising data: a critical reflection on the ‘hidden'issues,” *International Journal of Organizational and Collective Intelligence (IJOCI),* vol. 5, no. 1, pp. 1-15, 2015.

[5] P. B. Lowry and D. Wilson, “Creating agile organisations through IT: The influence of internal IT service perceptions on IT service quality and IT agility,” *The Journal of Strategic Information Systems,* vol. 25, no. 3, pp. 211-226, 2016.

[6] G. Whyte, A. Bytheway and C. Edwards, “Understanding user perceptions of information systems success,” *he Journal of Strategic Information Systems,* vol. 6, no. 1, pp. 35-68, 1997.

[7] M. Farsi, A. Daneshkhah, A. Hosseinian-Far and A. Chatrabgoun, “Crime data mining, threat analysis and prediction,” in *Cyber Criminology*, Berlin, Springer, 2018, pp. 183-202.

[8] T. Herath, H. Herath and W. G. Bremser, “Balanced Scorecard Implementation of Security Strategies : A Framework for IT Securi-ty Performance Management Balanced Scorecard Implementation of Security Strate-gies,” *Information Systems Management,* vol. 27, no. 1, pp. 72-81, 2010.

[9] V. Hooper and J. McKissack, “The emerging role of the CISO,” *Business Horizons,* vol. 59, no. 6, pp. 585-591, 2016.

[10] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb and S. Mahmood, “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study,” *Arabian Journal for Science and Engineering,* pp. 1-19, 2020.

[11] S. M. Abdullah, B. Ahmed and M. Ameen, “A New Taxonomy of Mobile Banking Threats, Attacks and User Vulnerabilities,” *Eurasian Journal of Science and Engineering,* vol. 3, no. 3, pp. 12-20, 2018.

[12] E. Brynjolfsson, “information assets, technology and organisation,” *Management Science,* vol. 40, no. 12, pp. 1645-1662, 1994.

[13] J. Magnusson, “Intentional Decentralisation and Instinctive Centralisation: A Revelatory Case Study of the Ideographic Organization of IT,” *Information Resources Management Journal (IRMJ),* vol. 26, no. 4, pp. 1-17, 2013.

[14] D. C. Cozmiuc and I. I. Petrisor, “Innovation in the Age of Digital Disruption: The Case of Siemens,” in *Disruptive Technology: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2020, pp. 1124-1144.

[15] J. L. King, “Centralized versus Decentralized Computing: Organizational Considerations and Management Options,” *Computing Surveys,* vol. 15, no. 4, pp. 319-349, 1984.

[16] H. A. Richardson, R. J. Vanderberg, T. C. Blum and P. M. Roman, “Does Decentralization Make a Difference for the Organization? An Examination of the Boundary Conditions Circumbscribing Decentralized Decision-Making and Organizational Financial Performance,” *Journal of Management,* vol. 28, no. 2, pp. 217-244, 2002.

[17] A. Khallaf and M. Majdalawieh, “Investigating the Impact of CIO Competencies on IT Security Performance of the U.S. Federal Government Agencies,” *Information Systems Management,* vol. 29, no. 1, pp. 55-78, 2012.

[18] R. Oppliger, “IT Security: In Search of the Holy Grail Oppliger,” ACM, 2007. [Online]. Available: https://cacm.acm.org/magazines/2007/2/5725-it-security/fulltext. [Accessed 2 Sep 2020].

[19] H. Jahankhani, A. Al-Nemrat and A. Hosseinian-Far, “Cyber crime Classification and Characteristics,” in *Cyber Crime and Cyber Terrorism Investigator’s Handbook*, Syngress, 2014, pp. 149-164.

[20] A. Hosseinpournajarkolaei, H. Jahankhani and A. Hosseinian-Far, “Vulnerability considerations for power line communication’s supervisory control and data acquisition,” *International Journal of Electronic Security and Digital Forensics,* vol. 6, no. 2, pp. 104-114, 2014.

[21] A. Cartwright and E. Cartwright, “Ransomware and reputation,” *Games (mdpi),* vol. 10, no. 2, p. 26, 2019.

[22] R. Collier, “NHS ransomware attack spreads worldwide,” *CMAJ,* vol. 189, no. 22, pp. 786-787, 2017.

[23] G. Dayanandam, T. V. Rao, D. B. Babu and S. N. Durga, “DDoS Attacks—Analysis and Prevention,” in *Innovations in Computer Science and Engineering*, Singapore, Springer, 2019, pp. 1-10.

[24] S. R. Curtis, P. Rajivan, D. N. Jones and C. Gonzalez, “Phishing attempts among the dark triad: Patterns of attack and vulnerability,” *Computers in Human Behavior,* vol. 87, pp. 174-182, 2018.

[25] M. El Mekawy, B. AlSabbagh and S. Kowalski, “The Impact of Business-IT Alignment on Information Security Process,” *International Conference on HCI in Business,* pp. 25-36, 2014.

[26] S. Laliberte, “Risk Assessment for IT Security,” *Bank Accounting & Finance,* vol. 17, no. 5, pp. 38-43, 2004.