Implementing converged security risk management: drivers, barriers, and facilitators

Title Page (including author(s) contact details)

Implementing Converged Security Risk Management:

Drivers, Barriers and Facilitators

Louisa Schneller, Cody Normitta Porter and Alison Wakefield

Correspondence concerning this manuscript should be addressed to Louisa Schneller, 44 U Pruhonu, Holesovice, Prague 7, 17000, Prague, Czech Republic. Email: louisa.schneller@teammacro.com

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators

Abstract

Converged security risk management is an approach that addresses interdependencies between security-related business functions that have traditionally been managed by separate departments within organizations. It is a more effective means of addressing organizational security risks and threats than tackling physical and information security challenges separately, given that the boundaries between the two are frequently blurred. However, fully converged security remains the exception rather than the rule, leaving organizations increasingly vulnerable as their adoption and reliance on digital technologies accelerates. Through interviews with eight senior security professionals, this research identified key factors critical to effective converged security risk management, expressed as 'drivers', 'barriers', and 'facilitators'. The practitioners' accounts illuminated how the modern threat landscape continues to drive further the need for such an approach, while the traditional separation of corporate security departments from the information security function in organizations remains a barrier. A greater focus on training and education, as well as soft skills, were identified as key priorities in the drive for an effective converged approach.

Keywords: Convergence, business continuity, enterprise risk management, soft skills, training, security management.

Introduction

The professional security community has actively promoted a 'converged' approach to organizational physical and information security management for around two decades, at the time of writing, which might reasonably be expected to have reached maturity by now. Reasons contributing to this apparent lag and how it may be alleviated are explored further below. Some of the earliest references to convergence are now difficult to source. For example, it was a recurring theme of the American periodical the *IOMA's Security Director's Report* going back to at least 1999, according to later editions (Seivold, 2007, 2012). The movement gained momentum in 2005, when the security associations ASIS International, ISACA and the Information Systems Security Association formed a coalition called the Alliance for Enterprise Security Risk Management, to promote such an approach and its recognition at organizations' board level. In order to examine the impact of convergence on global enterprises, the Alliance commissioned research from consultants Booz Allen Hamilton (2005), which conducted a survey and interviews with senior security professionals representing US-based global companies with revenues ranging from $1 billion to more than $100 billion. The findings depicted an ongoing shift from the functional separation of these two dimensions of security management, to one in which such activities were integrated to improve the value of the business. They reported the key drivers of these developments as being the rapid expansion of the enterprise ecosystem, value migration from physical to information-based and intangible assets, new protective technologies blurring functional boundaries, new compliance and regulatory regimes, and continuing pressure to reduce cost.

In their research for the ASIS Foundation, Beck, Gips and McFarlane Pierce (2019: 3) defined convergence as 'security/risk management functions working together seamlessly to address security holistically and to close the gaps and vulnerabilities that exist in the spaces

between functions'. In practical terms, this means that 'fully converged functions are generally unified and interconnected, reporting to one security leader', often having 'shared practices and processes, as well as shared responsibility for security strategy', so that they 'work together to provide an integrated enterprise defence'. The US government Cybersecurity and Infrastructure Security Agency (2021: 2) employs a more concise definition that draws attention to the inadequacies of an insufficiently collaborative approach, describing convergence as the 'formal collaboration between previously disjointed security functions'. Convergence forms part of an enterprise-wide approach to the management of risk (often referred to as 'enterprise risk management') and, within such a framework, the management of security risk ('enterprise security risk management') (Deloitte and Touche, 2006; CSO Roundtable, 2010; Willison and Sembhi, 2017; Allen and Loyear, 2019).

When the advent of computers marked the beginning of the journey from the industrial age to the information age, computer usage in organizations was mostly limited to data centres and their protection was focused on securing the physical infrastructure (Mutsaers, van der Zee and Giertz, 1998; Vermeulen and Von Solms, 2002). Technically, in the earliest days of organizational computing, converged security was the norm. The development of personal computers, new types of personal software and the expansion of chip technology (Mutsaers et a., 1998) led to their growing ubiquity in organizations from the early 1980s, increasing the potential damage of attacks and making organizational security much more complicated. The protection of IT systems required additional technical security measures, and it was from this point that information security began to evolve as a distinct business function and professional specialism (Vermeulen and Von Solms, 2002).

While the main benefits of IT advancement were initially to organizations' internal effectiveness, it became increasingly central to the realization of strategic business objectives,

for example, enabling the integration of the systems of suppliers and customers, and a matter for top management (Mutsaers, 1998). Through the 1990s, information and the IT systems to support it came to be recognized as critical business assets and gave impetus to the development of information security practices and standards (Vermeulen and Von Solms, 2002). The ISO 27000 family of international standards for information security (ISO/IEC, 2018), has its origins in the British Standard BS 7799, first published in 1995 by BSI Group, and has adapted to increasing legal and regulatory requirements associated with the protection of data in a fast-evolving information landscape. Since that time, computing power has multiplied many times over (see Schaller, 1997 on Moore's Law); the increasing ubiquity of digital devices has offered companies new ways of interacting with customers; and digital innovations like cloud computing, the Internet of Things (IoT) and artificial intelligence technologies are reconstructing how businesses function. A global survey of executives undertaken by McKinsey and Co. in July 2020, early in the COVID-19 pandemic, suggested that the challenges it had presented organizations, and necessary adjustments like the rapid expansion of home working, had already accelerated the adoption of digital technologies by several years. These factors have made organizations increasingly information-driven and transformed the nature and extent of the threats being faced. The pandemic required numerous adaptations to organizational security (Jun Jie, Sathesh and Jesmond 2020), including the designation of frontline security operatives in the UK as critical workers (Security Industry Authority 2020).

Today, IoT technologies are transforming society through the proliferation of smart platforms (e.g., homes, buildings, infrastructure, and cities) and the integration of digital, cyber-physical and social systems. At the same time, however, they present profound risk management challenges due to their complexity and the limitations of existing risk

management models and practices (Nurse, Creese and De Roure, 2017). The concept of Industrial IoT (IIoT) has entered the business lexicon to refer to its application to manufacturing and industrial processes, taking the risks to critical infrastructure to a new level. This urgency has been recognized by the US government, which established a Cybersecurity and Infrastructure Security Agency (CISA) in 2018, and in CISA's publication of a convergence guide in 2021. The guide advocates '[a]n integrated threat management strategy' reflecting 'in-depth understanding of the cascading impacts to interconnected cyber-physical infrastructure' (p.2), and views '[a] culture of inclusivity' as being 'vital' to the successful convergence of security functions and 'fostering communication, coordination, and collaboration' (p.3). The potentially disastrous outcomes should the security of such systems fail was illustrated in the cyber-attack on Silicon Valley start-up Verkada Inc. in March 2021. The hacktivist group claiming responsibility wished to show the ubiquity of surveillance in modern life and, in doing so, exposed sensitive footage from within hospitals, prisons, and 222 cameras within Tesla warehouses and factories, claiming to have footage from all Verkada customers (Turton, 2021). The potential for misuse of the available footage is significant, and the hacktivists highlighted not only the omnipresent nature of surveillance in today's society but also the vulnerabilities in modern networked security systems.

In the contemporary risk climate, it is unsurprising that an international survey of chief executive officers (CEOs), chief information security officers (CISOs) and chief security officers (CSOs) found that the CISOs were receiving more attention and funding than CSOs (Cilluffo, Smith and Cardash, 2019). The arms race between information security practitioners and cyber criminals has arguably now reached fever pitch. The fact that there are now thought to be 4.19 million cybersecurity professionals worldwide evidences the scale of demand for cyber security expertise, and it is estimated that a further 2.72 million

additional professionals are needed globally to enable organizations adequately to defend their critical assets ((ISC)^2, 2021).

It might reasonably be expected that the historic silos between physical and information security would by now have significantly broken down. However, the extent of the problem that remains was highlighted in the World Economic Forum's (2016) *Global Risks Report 2016,* which observed that 'While there are many "C" level owners (CISO, CFO, CEO, CRO, Risk Management), each of these owners has differing but related interests and unfortunately often does not integrate risk or effectively collaborate on its management' (p.78). The ASIS Foundation research (Beck, Gips and McFarland Pierce 2019) suggested that organizations, particularly large ones, have generally been slow to do this, constrained by confusion over who owns these risks and, therefore, whose role it is to manage them. It reported disappointingly low rates of what it termed 'full convergence' in the accounts of just 19% of over 1,000 executives from the United States, Europe and India who responded to the survey. Although the convergence of either physical or cyber security with business continuity management – the planning and preparation undertaken by organizations to enable them to restore their business functions following disruption – was more commonplace, reported in nearly half of the organizations surveyed.

The report's authors suggested that the lack of a singular definition or understanding muddied the findings. The research noted varied responses when security professionals were asked what the term meant to them. Indeed, a one-size-fits-all approach to convergence may not be effective or even possible (Booz Allen Hamilton 2005), given the varying requirements of different markets, industries and professions (Willison and Sembhi 2017). It needs to be customized to meet the requirements of unique organizations within specific lines of

business (Aleem, Wakefield and Button, 2013; Beck, Gips and McFarland Pierce, 2019). Gill and Howell (2016) emphasized that more research is required to move the conceptual into practical, particularly in understanding the different convergence approaches or models that may be employed. Related to this is importance of security practitioners regularly updating their learning, in new approaches to security risk management in general, and convergence approaches specifically (Aleem, Wakefield and Button 2013). Beck et al. (2019) cited confusion over roles and responsibilities, reporting lines and communication, as well as conflict among converged staff, as continuing barriers to the effective implementation of convergence.

Recruiting people with the right skill sets was identified by Beck et al. as being crucially important. Their findings suggested, however, that leadership of converged efforts could be based on 'culture, personality, relationships or even happenstance' (p.12) rather than leaders necessarily possessing the required business skills as well as soft skills ('the intangible, nontechnical, personality-specific skills that determine one's strengths as a leader, facilitator, mediator, and negotiator', according to Robles, 2012: 457). In earlier research on corporate security, leadership and strong communication skills were identified as essential means to ensuring organization-wide buy-in of the management solution (Briggs and Edwards, 2006). In its *Chief Security Officer (CSO) Guideline*, ASIS International (2013) emphasizes that, at a strategic management level, strategic, business, organizational positioning and interpersonal abilities are more critical than technical security skills. Brooks and Corkill (2014) also recognize practitioners' business understanding as being key to converged implementation, while a business-driven approach also ensures that the value-creating activities of an organization can continue (Aleem, Wakefield and Button, 2013). The implications of failure

are grave, as Beck et al. (2019) underscored, presenting the risk of missing key threats and failing to achieve full awareness of the organization's total risk position.

Research methodology

To gain a closer, qualitative understanding of the benefits and challenges in implementing an effective converged approach to corporate security, semi-structured interviews were conducted online via the Skype and Zoom platforms between February and March, 2020. Eight senior corporate security professionals from Europe, Australasia, and the Middle East (six male and two female) were interviewed, as detailed in Table 1. All of the candidates, bar one, who was approached directly, were selected from responses to a call for participants published on the professional social networking sites Linkedin and Twitter. Collectively, the participants were specialists across the fields of IT security, physical security, and business continuity. They represented both the private and government sectors, and a wide range of industry experience including, logistics, energy, cyber security and information technology, automotive, and national defence. One participant was also active in conducting research into practical security convergence. The participants were either responsible for actively setting up and/or maintaining converged approaches within their organizations, or they recognized that the principles behind convergence were present in their organization even if this approach had not been formalized. Their interviews were audio-recorded and then transcribed verbatim to allow for in-depth analysis.

Number	Sex	Position
P1	Male	Senior Corporate Security Practitioner
P2	Female	Senior Business Continuity Practitioner
P3	Female	Senior Corporate Security Practitioner
P4	Male	Senior Information Security Practitioner
P5	Male	Senior Information Security Practitioner
P6	Male	Senior Corporate Security Practitioner
P7	Male	Senior Corporate Security Practitioner
P8	Male	Senior Information Security Practitioner

Table 1: Career position and sex of participants.

Research findings

The research findings emerging from the participants' accounts were grouped into three main categories termed the 'drivers', 'barriers', and 'facilitators' of security convergence. 'Drivers' refers to the primary security and risk challenges that prompted or influenced the participants and their organizations to consider or implement a converged approach. 'Barriers' addresses elements identified by the participants as a limiting factor in its effective implementation or continuation. Finally, 'facilitators' represents factors that were identified as supporting the success of convergence.

Figure 1 presents a map of the three main themes and the sub-themes deriving from the data analysis and associated with each, which are discussed in turn.

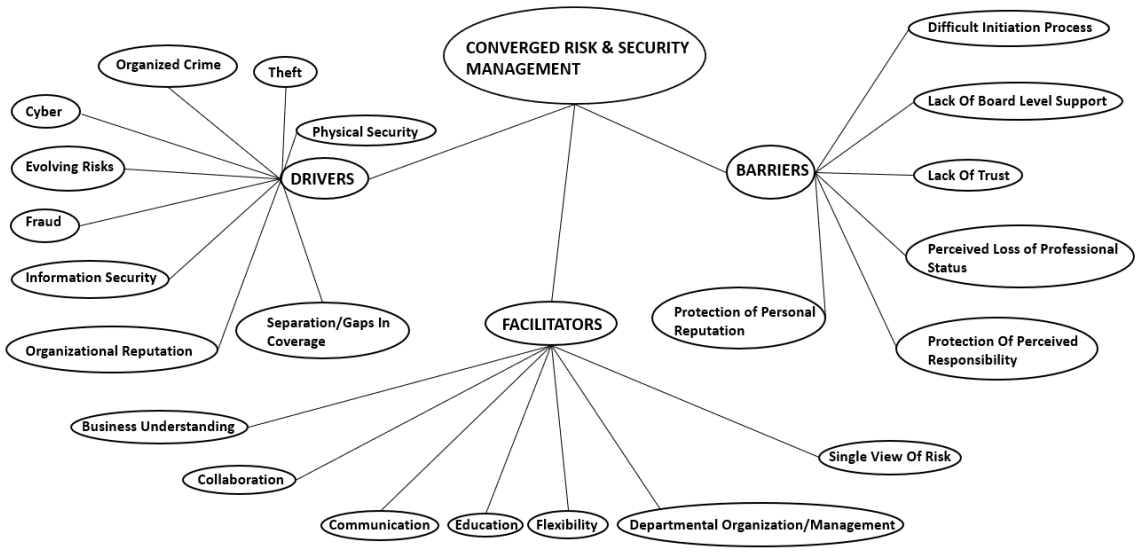

Figure 1: Thematic Map of perceived converged risk and security management themes and sub-themes.

Drivers

The future security challenges that most concerned the security professionals interviewed, termed the 'drivers', included cyber-attack, fraud, information and physical security, organizational reputation, and organized crime. The priority threats identified by the participants varied by their industry, so organized crime, for example, was a particular concern for just one of the interviewees owing to their involvement in the shipping sector. However, all but one spoke of cyber-attack as an issue requiring more attention, highlighting the extent to which this sphere presents ongoing and increasing security challenges for organizations

The concept of 'evolving risks' was also discussed by the research participants, highlighting the constantly changing risk and threat environment in which security professionals operate, and their need to remain abreast of this. The responses incorporated both simple and more complex articulations, for example:

The threats are always changing and that's the way it always is and always will be.

(P8)

> *So, I think there is high potential where quantum computing can have a very positive dimension, as you can make multiple tasks in a in a piece of a second but also you can really destroy security codes in the piece of a second (which really are quite secure at the moment.) And we rely on them, and the big question mark that I see as forthcoming is what happens if all these high security codes become insecure in the, let me say, a week or a day.* (P7)

Such implicit and explicit understandings of the ever-changing risk and threat landscape informed the security professionals' recognition of the need for an efficient way of addressing its management.

The final category within the drivers theme was 'separation/gaps in coverage'. This referred to responses in which the security professionals either specifically or unintentionally spoke of scenarios in which the delivery of security had failed, or would fail, due to the complete separation or lack of communication between various departments or organizations. Most security professionals raised such issues, whether it referred to the necessity of closing the gaps or the benefits of such gaps being eliminated. For example:

> *If you've got an incomplete view, you're only ever going to be distracted because you haven't got a whole view of risk.* (P8)

> *One of the problems with this is law enforcement agencies who fight crime are divided. For example, there so many agencies in the UK now all fighting the same thing.* (P1)

> *The biggest benefit is, of course, that if I look from the point of a customer, it's a one-stop-shop. So, for my customers internally, it doesn't matter on what security topic they have questions - they know they must go to group security. And if we have more the silo thinking they really have to think, 'OK, I have a topic about missing documents, or some data is open on the street, is this an information security topic? Is this a data protection topic?' (We know it's for both a topic), 'but where do I have to go?'* (P6)

The responses suggested that security professionals are aware of the pitfalls that organizational or departmental separation can cause, and the benefits that rectification of it can reap. It stands to reason, therefore, that the successful management of this separation is

still a driving force behind the delivery of an effective approach to converged risk and security management.

Barriers

The second major theme of the research was 'barriers', representing elements identified by the security professionals that, in their experience, actively contributed to the failure or impediment of converged risk and security management. The identified barriers ranged from traditional organizational roles through to the individual behaviours of those involved in the converged security management process or attempted implementation.

Half of the security professionals spoke of what was eventually categorized within the data analysis as the 'difficult initiation process'. They covered topics within these parameters that included the lack of organizational buy-in, and the difficulty in bringing disparate groups within the organization together in the first place. For example, one participant described the challenge of first managing and understanding their immediate role, and then having to bring together separate groups within an organization and externally, stating:

> *This takes time, to understand the bunch of topics that are in your area of control at the moment, and then you need to make a plan to get this done … And then you have a lot of interfaces internally and externally, for example, police, etc., state authorities, and internal, you have a whole bunch of functions like legal, internal audit, production and so on.* (P7)

Their comments illustrated how the process of implementing converged security management could be a personal challenge. Other interviewees echoed this view, for example, one commented:

> *I expect from my managers that if they have a topic, that they oversee the whole issue, and that they get their colleagues from the same department (but working maybe on different topics) to get on board … But that's also the challenge.* (P6)

The security professionals also described the difficulty in trying to corral groups and roles

within their organizations that were traditionally separated within the organizational culture.

> *It's very hard to get buy-in from all the areas of the organization at the moment ... It's not a concept that's well understood … I tried to get the IT and cyber to work closely with the rest of security, but that was very difficult. Competing budgets is very difficult. Different people with different skill sets and being focused in their own silos is very hard to break down. (P1)*

> *The main challenge is to get them all on board. Because every department is its own small kingdom … it's a little bit like the US …. everybody has his own state, and now we say, we make you the United States and at the end there's one person who's managing this complete department and of course everybody is doing their own tasks … but at the end, the one who is then in the management team or at least the CSO on top, he has to manage that they get in contact with each other still. (P6)*

The participants intimated that, in their experience, a lack of trust within their organizations had also created barriers to the effective delivery of converged risk and security management. They cited a lack of trust both from within and outside the organizational security department as a barrier to success. For example, one security professional recalled a previous chief security officer's refusal to trust their colleague's abilities and professional specializations.

> *The other one we had before was only on paper, doing the pointing and doing the telling. It does not work like that.* (P3)

However, it was also clear that this lack of trust extended beyond the security group. Another security professional described how the trust of those within the organization, yet outside the security group, could become a barrier:

> *But this is, I think, the major part, that management could say that "oh this is ridiculous, is the CSO really able to do the cyber stuff? Is he knowledge-wise good enough to deal with a whole bunch of topics that could be a hurdle to overcome?" and then someone has to let loose.* (P7)

The evidence illustrated how hard security practitioners must work to build trust within their own department and secure the confidence of those outside the security department, particularly within departments in which converged security was actively sought.

Individual personal factors were also identified as barriers by the security professionals, pertaining both to those trying to implement converged security management,

and those with whom they had to work while implementing it. The comments gathered showed how a perceived loss of professional status could affect the engagement of both groups. For example, one security professional spoke of the reticence that may be felt by a chief security officer (CSO) if they are concerned that failure might affect their professional status.

> *A lot of CSOs doubt in themselves, "Am I the right person to hold such a bunch of topics?" Some say, "I don't want to touch this because if I do not get the green light to get it done, will I burn myself with the organization with this attempt?* (P7)

They also spoke of a similar feeling in those who did not want to cooperate with the CSO:

> *First you will not have the buy-in of other partners, for example, the CIO* [Chief Information Officer] *does not want to get rid of the topic because they say, "cyber security is an important topic of the future and I want to have my stake in it.* (P7)

This view was echoed by other interviewees:

> *And then you've got the physical security people thinking that these cyber people are after their jobs.* (P8)

Plausibly, the participants may have felt that a fear of the loss in status on both sides could also potentially be a barrier to successful converged security management.

The collected evidence regarding barriers shows multiple factors that the security professionals considered important. Traditional groups or silos within organizations can be difficult to break down and the personal challenge required to do this can be considerable. Meanwhile, fears regarding the loss of professional status can plague both the practitioner seeking to implement a converged response, and those with whom they seek to work.

Facilitators

The security professionals also identified factors placed under the heading of 'facilitators' that, according to the professional's experience, contributed in some way to the success of a converged approach to security. These ranged from desirable personal skills, to

how security and risk management are conceptualized and, finally, the practicalities of an effective organizational structure.

All the security professionals identified multiple beneficial skill sets. Six of the eight interviews spoke of the need for practitioners to have a strong business understanding to be personally effective, gain support from other areas of the organization, and help mitigate the barriers described above. For example:

> *That means you understand the balance sheet, that means that you have to understand the organization, and that varies across every organization that you work in. It means you've got to understand financial statements. It means you've got to understand the regulatory market. It means you've got to understand the complexities of an organization. Its footprint. Its geography and all these things. At the same time, you have to understand the impact, the likelihood, the severity of a cyber-attack on that organization and what it can do to that organization.* (P4)

> *Because we know, for instance, that in emergency planning, we know that every $1 that you spend in preparedness and planning returns you 4 in response and recovery. It's a hell of a good return of investment … So, you mention that to a CFO* [Chief Financial Officer] *and, my goodness, their ears prick up. That's a hell of a return on investment. So, do you want your organization to be insecure and then be on the backfoot trying to secure it, or do you want to make it more resilient and stronger in the security space so it doesn't fail.* (P2)

> *And then the other side is being part of in part of the business, the advantage is you can get buy-in. You're able to sell stuff to the business. As an important thing.* (P4)

All the security professionals spoke of the need for strong communication skills, once again identified as being necessary to help alleviate specific barriers. For example, one interviewee referred to the need to be able to communicate convincingly at board level.

> *You know, having a conversation with the CEO about security and talking about technology is not going to get you very far. And it's proven to not get you very far. You know, there's so much material out there, research out there that says boards don't 'get' security. And there's a really good reason why they don't 'get' security … Why don't they get security? Because security doesn't talk the board language. And the board invariably has a 'what's in it for me?' mentality.* (P4)

Strong communication skills were also identified as being essential for the practitioner to overcome a lack of inter-organizational trust, as another participant described:

> *I think you need to present them really the synergies and benefits coming out of that so that they can really weigh it and measure the whole stuff. Then they become most probably convinced.* (P7)

Another key facilitator identified by the research participants was the concept of collaboration, referring to the need for security practitioners to move beyond the boundaries of their role within the group or organization. As one interviewee observed:

> *You can specialize in one area but must also take into consideration other parts of security specialisms that may not be clear to you, that you're not clearly an expert in but you know where to go to get further information.* (P5)

The security professionals also noted that the convergence of threats made collaboration an unavoidable necessity, another stating:

> *It was very separated before and* [now] *we are touching each other more and more with what we are working on.* (P3)

> *I think it's important that both do get the other one. The current CISO is understanding that my world is different and that other things are going on at my side, and that I do understand that as well from his side.* (P3)

Other personal skills mentioned both directly and indirectly by the security professionals as mitigating barriers to convergence included flexibility and leadership. These were seen to enable the practitioner to cross-departmental boundaries within the organization and secure buy-in. Flexibility was described by one interviewee as providing a way to cross gaps in security coverage, and facilitate collaboration and communication:

> *You can specialize in one area but must also take into consideration other parts of security specialisms that may not be clear to you, you're not clearly an expert in, but you know where to go to get further information.* (P5)

Half of all security professionals discussed leadership directly and emphatically, one elaborating:

> *Having the right leadership regardless of your background and being open-minded. I think the days of scaring people are long gone if that's the only tool you have. So, I think it's having that strong leadership. Being able to make decisions and be accountable for your decisions, but at the same time grow the business, whatever*

business you're in. (P5)

Another highlighted that the removal of strong leadership could have a detrimental effect on converged security.

> *In a lot of companies, it's really depending on the person in charge. For example, if someone who has a converged model leaves the company, there is a big chance that the board goes backwards instead of continuously forward.* (P7)

Having a single view of risk and threats was identified as both a conceptual and practical necessity in the effective deployment of converged security management and a further facilitator, with two interviewees commenting:

> *Some people do practice it. I've seen people with similar backgrounds to me seeing the threats as one and therefore working out the best way to do it and therefore using all assets, people, infrastructure, etc. to defeat the threats. But it's not well understood at board management level.* (P1)

> *Converged security management really does involve, as I said, a single view of risk, and taking actions as a result of that single view. And it does mean being able to do something about it. It doesn't just mean it's an academic exercise where you know what the risks are, and you can't do anything about them.* (P8)

Another factor identified was departmental organization. No single organizational model was perceived by the security professionals as the sole or best method of practising convergence, but it was indicated that barriers could be avoided by using a more collaborative organizational approach. For example:

> *What I have also seen is like a hybrid model, let's say, this IT security, this cyber security, we still have the physical security. But you have like a security board where they come together. Discuss the topics with each other, taking partly over or supporting each other, then go out again and do all their own thing again.* (P6)

Another interviewee expressed a preference for the complete merging of departments, while acknowledging that this may not be possible:

> *For me, it means bringing both cyber, all security domains in one function. Or if that is not the case for organizational reasons, at least to have a holistic governance view*

on all topics and not to do it in silos. (P7)

While the participants expressed no universal preference for an organizational model, it was clear that whatever method was chosen, including complete merging or a more holistic and collaborative approach, it needed to be clearly defined. This view was evidenced by the following statement:

> *With all these different teams, what you end up having is different people, different responsibilities, where some of them know what they're responsible for and what's right for them to be responsible for, and yet there's others, other things that go on where no-one knows who's responsible. And because no-one knows and this hasn't been clarified, that's where you end up with situations.* (P8)

Education and training were identified as a key facilitator by just over half of the security professionals. Their importance in shaping essential business and communication skills in the security practitioner was reflected in the following comments:

> *Those who practice risk management security need to become better educated and portray their message to the board and the budget holders in a way that they describe the problem* [and] *how they're going to resolve it as being of benefit to the business, they get a return on their investment if you like, and therefore it's much more conducive to being successful to fighting the various threats.* (P1)

From the data collected related to education, two participants identified a lack of convergence-specific education or training:

> *I think firstly, the whole concept of a converged approach to security and risk management, as you say, is that the way it is taught at the moment and the way it is trained. They are trained in silos. So courses are there to do risk management or business continuity planning, or physical security and access control. They're all taught separately. This concept is not widely understood.* (P1)

> *I see a trend and I know, get to know, more and more CSOs who have studied this. But we are still in the big minority compared to the overall populations.* (P7)

A third professional noted a lack of training in keeping with the evolution of modern security overall.

> *I think one of our biggest challenges is staffing and school shortages. It's all very well to go to AI, but do we have the right people to programme it, do we have enough of these people? Many organizations seem to have a large number of what I call single*

> *points of failure, which is a business continuity term, and not enough people to do something, that's very critical, and what the hell happens if it's not available on short notice?* (P2)

Discussion

For today's organizations, security threats are increasingly converged, and require a converged approach to risk and security management that adopts a single view of risk. The literature highlights the need for effective converged security management in an increasingly complex operational environment (Azeem, Wakefield and Button 2013; Willison and Sembhi 2017; Beck, Gips and McFarland Pierce 2019) in which traditional approaches are no longer wholly effective, particularly considering the increasing reliance on IoT and cloud computing technologies and the new risks these present (Nurse, Creese and De Roure 2017). Recognition of the criticality of managing these convergent threats is not new (Schultz, 2007). However, new security challenges such as those presented by the COVID-19 pandemic (McKinsey and Co., 2020; Jun Jie, Sathesh and Jesmond 2020), and recent security breaches such as the Verkada cyber attack of March 2021, clearly demonstrate the vulnerability of this increasingly interconnected environment (Turton, 2021), and our findings support this. Senior security professionals participating in the study typically identified the need for a single view of risk encompassing all areas of the organization, and mitigating vulnerabilities caused by increasing interconnectedness and converging threats. All the participants, who were interviewed before the global lockdowns and the changes they brought with them had fully taken effect, recognized multiple security risks to their respective organizations, and acknowledged that the threat landscape was constantly evolving. They viewed converged risk and security management as an essential means to achieving this.

Both the literature and our data reflect how, despite widespread recognition of its importance, converged security management is yet to become the norm within organizations.

For the better part of a decade, low implementation rates have been reported (Seivold, 2012; Beck et al., 2019), and more research is required to promote this, particularly in understanding the different approaches or models that may be used (Gill and Howell, 2016). This research does not consider convergence to be an unqualified good, rather, the approach has been interpreted as beneficial when deployed effectively. The participants in our research recognized these challenges, identifying multiple practical barriers to its implementation, and key facilitators of success. Significant among the facilitators was strong soft skills in senior security practitioners effectively promoting convergence within their organizations. Leadership and strong communication skills were identified in the literature as means to ensuring organizational-wide buy-in of the management solution (Briggs and Edwards, 2006), and the research of Beck et al. (2019) noted that the lack of it led to confused lines of reporting and even personnel conflict. This was also reflected within our findings, with one security professional describing a scenario whereby, if a strong security leader left the organization, there was no guarantee that a converged security management model would continue. It seems inarguable that key skills such as leadership, communication, flexibility, and collaboration will aid effective converged implementation. Since no workable single standard model of converged security management exists (Booz Allen Hamilton 2005; Aleem, Wakefield and Button, 2013; Gill and Howell 2016; Willison and Sembhi 2017; Beck, Gips and McFarland Pierce, 2019), it is perhaps no surprise that soft skills are being relied upon to sell and maintain convergence within the organization. Perhaps moves by government organizations such as the US government's Cybersecurity and Infrastructure Security Agency to recommend cyber and physical convergence (CISA, 2020) will promote a more codified approach, however, in the meantime, such skill sets must be actively cultivated by the security practitioner and wider profession to secure organizational buy-in and effectively manage security across often disparate units within organizations.

Consistently, interviewees suggested that further training and education could promote wider implementation of converged security management, a point that was acknowledged somewhat in the examined literature (Aleem, Wakefield and Button, 2013). The emphasis placed on business skills within the literature (Briggs and Edwards, 2006; ASIS International, 2013; Brooks and Corkill 2014; Engemann 2018) was also echoed by six of the eight interviewed security professionals, as it enables the practitioner to speak the language of the board to ensure buy-in. Considering that recommendations made years ago were still highlighted as issues in the interview data, it is evident that the security profession still needs to meaningfully address these factors. Extending training and education in converged security, business understanding, and wider soft skills will be essential for convergence fully to be realized.

Conclusion

While a conceptual understanding of a converged approach to risk and security management is prevalent, the practicalities of implementing it still presents challenges to its practitioners. From the data gathered and analyzed it is clear several themes are particularly relevant to security management convergence and its effective implementation. First, the evolving threat landscape, calling for a single view of risk, is making a converged approach to risk and security management more of a necessity. Secondly, strong business skills as well as softer skills such as strong communication, flexibility, and leadership skills are critical requirements for the security practitioner if the approach is to achieve buy-in from all areas of their organizations, particularly the board level. Finally, it is possible that broader implementation has been slow because converged management suffers from a lack of specific training available to practitioners. Silos need to be broken, not just organizationally, but in how security is taught. Practically, the industry might consider hiring from as diverse a pool of candidates as possible to ensure a greater breadth of experience and amending standard job

descriptions to have a stronger focus on softer skills. These recommendations may go some way to broadening the industry skill sets and knowledge base required to approach convergence more effectively.

References

Aleem, Azeem, Alison Wakefield, and Mark Button. 2013. "Addressing the Weakest Link: Implementing Converged Security." *Security Journal* 26, no. 3: 236-248.

Allan, Brian, and Rachelle Loyear, 2019. *Enterprise Security Risk Management: Concepts and Applications*. Brookfield, CT: Rothstein Publishing.

ASIS International. 2013. *Chief Security Officer (CSO) Guideline.* Alexandria, VA: ASIS International.

Beck, David., Michael Gips, and Beth McFarland Pierce. 2019. *The State Of Security Convergence in the United States, Europe, and India.* Alexandria, VA: ASIS Foundation.

Booz Allen Hamilton. 2005. "Convergence Of Enterprise Security Organizations." *ASIS International Conference 2005.* Alexandria, VA: Alliance For Enterprise Security Risk Management.

Briggs, Rachel, and Charlie Edwards. 2006. *The Business of Resilience.* London: Demos.

Brooks, David J., and Jeff Corkill. 2014. "Corporate Security and the Stratum of Security Management." In *Corporate Security in the 21st Century: Theory and Practice in International Perspective*, edited by Kevin Walby and Randy K. Lippert, 216-234. London: Palgrave Macmillan.

BSI Group. 1995. *BS7799 Code of Practice for Information Security Management*. London: BSI Group.

CISA. 2021. *Cybersecurity and Physical Security Convergence*. Cybersecurity and Infrastructure Security Agency. Accessed 3 November, 2021. https://www.cisa.gov/cybersecurity-and-physical-security-convergence.

Cilluffo, Frank, Margaret W. Smith and Sharon L. Cardash. 2019. Cyber and Physical Security: Perspectives from the C-Suite, Survey Research Project. Auburn, AL: Center for Cyber and Homeland Security and International Security Management Association.

CSO Roundtable. 2010. *Enterprise Security Risk Management: How Great Risks Lead to Great Deeds. A Benchmarking Survey and White Paper*. Alexandria, VA: ASIS International.

Deloitte and Touche (2006) *The Convergence of Physical and Information Security in the Context of Enterprise Risk Management*. Alexandria, VA: Alliance for Enterprise Security Risk Management.

Engemann, Kurt J. 2018. “Developments in Risk Security.” In *The Routledge Companion to Risk, Crisis and Security in Business*, edited by Kurt J. Engemann, 3-19. London: Routledge.

Gill, Martin, and Charlotte Howell. 2016. *Tackling Cyber Crime: The Role of Private Security.* Tunbridge Wells: Perpetuity Research & Consultancy International (PRCI) Ltd.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2018. *ISO/IEC 27001:2018 - Information Security Management*. Geneva: International Organization for Standardization/International Electrotechnical Commission.

Jun Jie, Ng, Navaretnam Sathesh, and Lee Jesmond. 2020. “Considerations for IT Management in a Covid-19 World.” *IEEE Engineering Management Review* 48, no. 3: 16-18.

McKinsey and Co. 2020. How COVID-19 Has Pushed Companies Over the Technology Tipping Point—and Transformed Business Forever. Accessed 3 November, 2021. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

Mutsaers, Ernest-Jan, Han van der Zee, and Henrik Giertz. 1998. “The Evolution of Information Technology.” *Information Management and Computer Security* 6, no. 3: 115-126.

Nurse, Jason R.C., Sadie Creese, and David De Roure. 2017. “Security Risk Assessment in Internet of Things Systems.” *IT Professional* 19, no.5: 20-26.

Robles, Marcel M. 2012. “Executive Perceptions of the Top 10 Soft Skills Needed in Today’s Workplace.” *Business Communication Quarterly* 75, no. 4: 453-465.

Schaller, Robert R. 1997. “Moore’s Law: past, present, and future.” *IEEE Spectrum*. June: 52-59.

Schultz, Eugene E. 2007. “Risks Due to Convergence of Physical Security Systems and Information Technology Environments.” *Information Security Technical Report,* no. 12: 80-84.

Security Industry Authority. 2020. *Covid-19 and the Private Security Industry - FAQs.* London: Security Industry Authority.

Seivold, Geoff. 2007. “C-Level Contact is Greater in Merged Security IT/Security Depts.” *IOMA’s Security Director’s Report.* New York: Institute of Management and Administration.

Seivold, Geoff. 2012. “Value Promised by Physical and IT Convergence Going Unrealized.” *IOMA’s Security Director’s Report.* New York: Institute of Management and Administration.

Turton, William. 2021. “Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals.” *Bloomberg*, 9 March. Accessed 3 November, 2021. https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams.

Vermeulen, Clive, and Rossouw Von Solms, 2002. “The information security management toolbox – taking the pain out of security management.” *Information Management and Computer Security*, 10: no. 2: 119-125.

Willison, James, and Sarb Sembhi. 2017. *Supporting Enterprise Security Risk Management: How Vendors Can Support ESRM And CSM Strategies.* Kent: Unified Security Limited.

World Economic Forum. 2016. *The Global Risks Report 2016.* Geneva: World Economic Forum.

20th October 2021

Security Journal

Martin Hill, Editor in Chief

Re: Implementing Converged Security Risk management: Drivers, Barriers and Facilitators

Thank you for accepting our manuscript for publication in the *Security Journal*. We would like to thank you and your reviewers for feedback. We believe we have addressed the remaining proofing issues and the manuscript should be ready for publication now.

We hope these amendments now satisfy your requirements for publishing in the *Security Journal* and we look forward to hearing from you in due course.

Best wishes,

The Authors.

We have received the reports from our advisors on your manuscript, 'Implementing Converged Security Risk Management: Drivers, Barriers and Facilitators', submitted to Security Journal. Based on the advice received, I have decided that your manuscript can be accepted for publication after you have carried out the corrections as suggested by the reviewer(s). Below, please find the reviewers' comments for your perusal. One of the referees has also suggested that you need to make clear what is new about your work and perhaps provide stronger support for drawing conclusions from so few interviews.

We thank you for your comments and believe we have now addressed these concerns.

While submitting, please check the filled in author data carefully and update them if applicable - they need to be complete and correct in order for the revision to be processed further.

We have checked this and clarified all author information.

Reviewer #1: This is a timely topic. You do a good job of covering and explaining the relevant literature. A few important pieces seem to be missing, however. Most notably Gill and Howell's Tackling Cyber Crime: The Role of Private Security (2016) https://perpetuityresearch.com/wp-content/uploads/2016/09/SRI-Report-2016.pdf. Another one is Schultz, Convergent Security Risks in Physical Security Systems and IT Infrastructures (AESRM, 2006).

We agree and have added both articles to the manuscript on page 6, 19 and 20 (Gill and Howell). We were unable to locate the Schultz source, however we have added reference to Schultz, Risks Due To Convergence of Physical Security Systems and Information Technology Environments (2007) to page 19. We hope that its inclusion as well as multiple new sources have adequately addressed this concern.

Also, please check the ASIS Beck citation. I've seen it elsewhere as Beck, Gips, and McFarland Pierce.

We have changed this throughout the manuscript.

On the merits, I'd like to see a clearer explanation of what's new in this research and how it builds upon the earlier research--or else calls any of the previous research into question.

We believe that this has now been addressed through a stronger introduction section and discussion section. The research seeks to examine and build on the earlier research.

The last significant thing is that this research considers convergence as an unqualified good--as do the AESRM publications of the mid-2000s. But not everyone agrees. Just like all corporate risk (litigation, process, financial, reputation, IT, security, business, operational, etc) rarely feeds to a single person (besides the CEO), some argue that security risk is too broad or varying to

report to just one person. For example, the chemical industry, which is driven by safety mandates and concerns, often conjoins safety (including fire safety) and physical security and separates other aspects of security because they don't fit into that paradigm. Did any of the interviewees mention that? It seems to have come up in previous studies that you cite.

We agree that this should be reflected upon and have done so on page 20 of the discussion. Unfortunately, none of the interviewees mentioned this.

On a more minor note, there are a few typos, sentence fragments, and grammatical errors that can be cleaned up.

We apologise and have had the manuscript proofread externally.

Reviewer #2: INTRODUCTION

Page 2 line 3 - Introduction.
"A converged approach to security management has been put forward as a beneficial method of managing organizational security" Very passive for an opening statement, I'd prefer to see some metrics along the lines of who is putting this forward, where the comments are coming from, even some "X articles between 2019 and 2021 were written on this" or "Social Media mentions of this trended X between X and X" Something more concrete as the basis for an entire paper. I am not convinced by the opening that this has the traction claimed.

We agree that the opening statement was too passive, and this has now been changed on page 2.

Page 2 lines 45 - 50
The references claiming that convergence is not happening are all older than 2020. The impact of the COVID pandemic on the digitization of security and the defacto convergence of systems to the cloud make these older references stand out. It would be nice to see a newer reference that makes it clear that this is still a highly impactful and relevant problem post the initial COVID resilience responses across industries.

We agree and the application during covid has been reflected upon in the discussion. See pages 4 and 19.

Page 4 Line 1
"expected this year to reach 24 billion,"... I know this is a frequently updated statistic. Could

say "expected to reach X by 2022 (or 2023) so that the reader knows the timeframes referenced.

We agree and although we have removed this sentence, we feel that pages 4-5 now more fully inform the reader of the scale and application of IoT systems today and how this impacts the need for better security and more practitioners.

General introduction note. I wonder if the author might consider tying some aspects of the introduction more strongly to "This item is explored further in the research findings" or "this statement is supported further by the data collection process that the author undertook. The intro is overall a very strong argument in support of needing converged security management. But I would like to have some foreshadowing of the findings tied into the intro.

We agree and have added this in the introduction.

FINDINGS

General comment on findings section- Perhaps get permission from the participant whom was quoted often with "ums" and some repetition to "clean up" the direct quote? I do understand that it makes it very clear that it is their own wording, but is a little distracting for the reader.

We agree and have cleaned each quote.

Very strong examination of the findings! There was some interpretation on the Authors part but it all seemed to be fully supported by the direct quotes and no conclusions were made that this reviewer found to not be supported by the content quoted from the study participants.

Thank you.

DISCUSSION

Page 19 line 20
"Recent security breaches such as the Verkada hack of March 2021 clearly demonstrate the vulnerability of this increasingly interconnected environment (Turton 2021). They also demonstrate that the threats themselves have become converged (Booz et al., 2005). Our findings support this"
This reviewer would like to see a little more supporting content. Perhaps some commentary about Industrial IoT and Cloud Based Ops and the push to digitize many aspects of the business.

We agree and more supporting content has been added on pages 4-5. Per your suggestion we have also added some commentary about cloud-based computing and its reach across all sectors, in particular critical infrastructure.

The discussion makes several points that this reviewer AGREES with, but the de facto statements could use some additional supporting examples to drive the point home.

We agree and have added more support throughout the manuscript.

CONCLUSION

Conclusion was very strong.

It may be outside of the intended scope of the paper, but if it could be contained within the rubric, some "what does the security industry as a whole need to do" commentary would be a welcome addition to the document. ex: updating standard job descriptions to include softs skills, making more robust certifications? I would have been interested in the authors opinions on what to do with the research at the industry level.

We agree that some commentary was needed, and this has been added to the end of the conclusion.