Toward a disciplined alignment in information security management

Kengo Zenitani
Department of Mathematical and Computing Science, School of Computing, Institute of Science Tokyo, Tokyo, Japan

Received 16 October 2022
Revised 22 July 2024
3 June 2025
Accepted 19 August 2025

Abstract

Purpose – This article examines the data breach that occurred in the Office of Personnel Management (OPM) in the US federal government to discuss the issues in information security management. The US federal government had the law and plenty of carefully examined guidance and information security management practices were mandated under them. Thus, the lack of a managerial framework was not the problem. This article tries to elaborate on the issues inherent in the current practices and propose a research program to overcome them.

Design/methodology/approach – We examine the OPM data breach to identify the issues in information security management. This leads to the identification of the following three issues: insecurity in risk analysis, distance from business risk analysis and alienation from corporate governance. Then, we refer to several relevant pieces of research to see how well those efforts help solve the issues. Subsequently, we enumerate three gaps between information security research and practices which inhibit the productive collaboration of researchers and practitioners.

Findings – The misalignment of risk conceptions between security and business practitioners is pointed out as the critical factor in catastrophic failures. In addition, the concept of misalignment is also applied between information security researchers and practitioners. The reconciliation of this variety of misalignments shall contribute to rational information security management.

Originality/value – A draft research program is proposed to overcome these issues and to build mutual trust among various parties. This program puts emphasis on secured risk analysis that is robust against the conflicts between business and security practitioners.

Keywords Risk management, OPM data breach, Information security management system, Information security risk analysis, Disciplined alignment

Paper type Conceptual paper

1. Introduction

Information security and its management is one of the vital issues in today's world. Many best practices and techniques are developed for the topic. These tools enable us to protect ourselves from malicious attacks, in theory. In reality, it is not uncommon to see large-scale security breaches happening in industry and public sector. To understand the situation, let us see a case in the Office of Personnel Management (OPM) (Committee on Oversight and Government Reform, 2016).

The OPM is a federal government agency in the USA. The agency implements federal human resources policy, oversight and support for federal government employees, retirees and their dependents. On July 4, 2015, the OPM disclosed that it was found to be attacked by an unknown attacker and over twenty million personnel records, including the background investigation results of counter-terrorism officials, were breached. Michael Hayden, the former director of the CIA, said that "[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it" [1]. The OPM data breach is one of the most severe incidents in history. In contrast to

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 6 No. 1, 2026
pp. 32-51
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-10-2022-0019

Mr. Hayden's argument, the report cannot show clear evidence of the culprit. It only enumerates circumstances, as is often the case in this sort of attack. This anonymity of the attack even emphasizes the shock of this unprecedented incident and its aftermath.

The OPM officials were not without tools to prevent the incident. For example, it was pointed out later that if an integrated circuit (IC) card-based authentication, which was standardized and promoted in advance, had been introduced earlier, the intrusion could have been prevented. Also, the US federal government has published many guidelines called the SP-800 series (NIST, 2008, 2011, 2012, 2013, 2014, 2018) for federal information security management to comply with the Federal Information Security Management Act (PL 107–347). That is, they had an enforcing law, detailed implementation guidelines and a technical solution to establish their security.

The critical factor behind this catastrophic result was strong pressure on their business. After the 911 terror attacks, the U.S federal government, vigorously promoting counter-terrorism policy dramatically increased the number of relevant personnel. "That staffing surge caused a backlog in processing background investigations. The backlog was at least 188,000 by 2004. The Intelligence Reform and Terrorism Prevention Act (PL 108–458) required that 90% of clearance applications had to be resolved within 60 days by 2009, a reduction of 84% from the then 375 days average wait time" [2]. Additionally, it was decided around the end of 2004 to consolidate to the OPM the relevant investigation tasks previously held in other departments and agencies. As a result, "it is not uncommon for existing policies to be circumvented in order to achieve business functions while exposing the entire agency to unnecessary risk" [3].

The OPM data breach is not a singular case. On June 1, 2015, the Japan Pension Service (JPS) announced that about 1.25 million records of privacy information had leaked out by an advanced persistent threat (Investigation Committee on Information Leakage due to Unauthorized Access, 2015; Verification Committee for the Incident of Information Leakage due to Unauthorized Access at Japan Pension Service, 2015; National Center of Incident Readiness and Strategy for Cybersecurity, 2015). This incident was also technically preventable; the breached information was assumed to be kept in the environment isolated from the internet. However, it was duplicated onto a shared file server accessible from the internet to ensure business efficiency. Japan's government had plenty of guidelines too and the JPS had appointed several officers as information security authorities. It is interesting to note that the JPS was established for swift and proper management of the enormous amount of pension records. It was rooted in a political event known as the pension record problem, in which a significant amount of records were lost due to inappropriate operation and the JPS was, like the OPM, naturally under strong pressure as a result.

Both cases indicate serious issues in information security management. First, poor management, not technical issues, caused both problems. Second, management guidelines and strong regulations on information security were in place. Third, despite these circumstances, business operations took precedence over information security. This is nothing but a failure of information security management. Technical measures and codified best practices never make a difference if people are indifferent to implementing them.

This concept paper's discussion unfolds in three principal stages. Initially, Section 2 clarifies the misalignment in risk conceptions between business or managerial stakeholders and security practitioners. This paper hypothesizes that such misaligned risk conception is the critical factor in catastrophic failures. Subsequently, Section 2 examines academic research offering potential pathways to address this divergence. Section 3 then addresses three communication gaps – analyzed as forms of misalignment – between researchers and practitioners. It also proposes strategies, primarily from the researchers' perspective, to facilitate the effective translation of research findings into practice. Such translation, in turn, offers an opportunity for academic research to contribute to reconciling the misaligned risk conceptions identified in Section 2. Finally, Section 4 proposes a draft research program designed to reconcile these intertwined misalignments. This multi-disciplinary program

would fuse insights from information security management standards, algorithmic risk assessment, enterprise architecture (EA), benefits realization management (BRM), project portfolio management (PPM), information security governance, systems engineering and the psychology of information security practices. Figure 1 depicts the structure of our discussion.

This concept paper aims to stimulate discussion and critical analysis of this proposed approach. While the author acknowledges limitations in his expertise and the potentially unfinished nature of this work, it represents an attempt to consolidate established research and best practices within the field. The primary focus is introducing a new perspective that may warrant further academic scrutiny and debate. The proposed research program intends to tackle issues in the managerial mechanism from the standpoint of (1) the misaligned risk conception by introducing tools with theoretically assured properties and (2) facilitating practical communication between practitioners and researchers. Through this two-faceted approach, the research program seeks to mitigate the types of failures exemplified by incidents such as those at OPM and JPS by presenting a mechanism actively fostering the aligned behavior of business and security practitioners.

Management standards, as compilations of best practices rooted in practitioner consensus, do not inherently carry scientific validation for their immediate effectiveness. It is

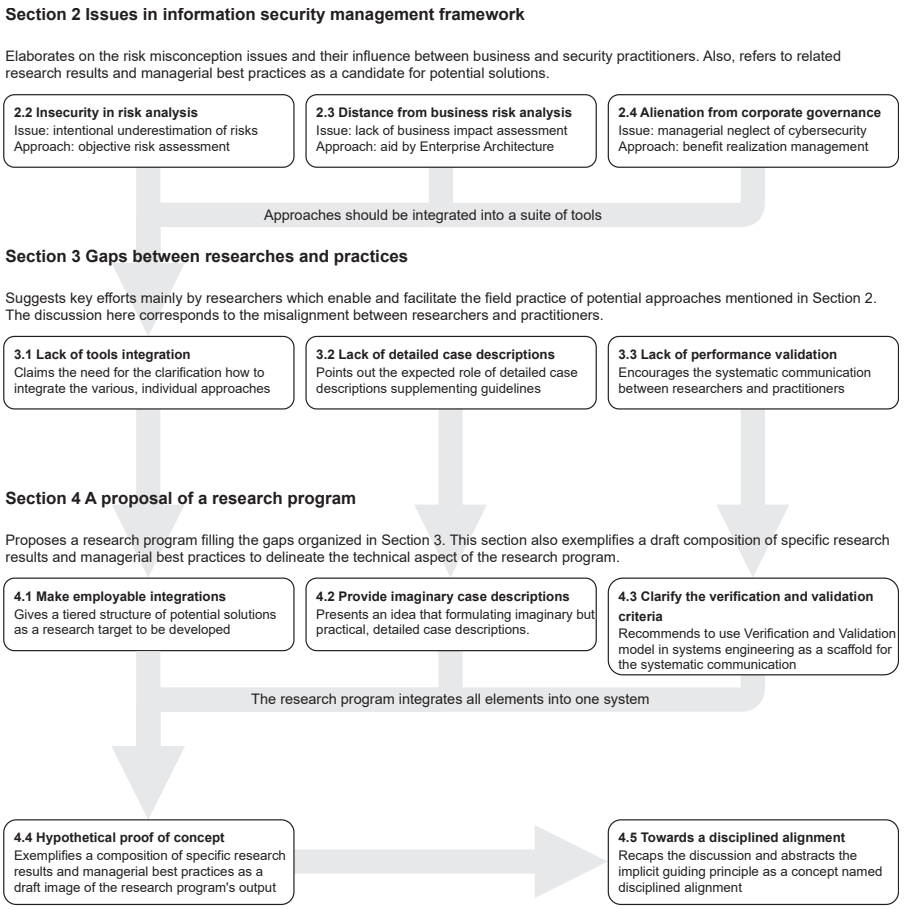

Figure 1. The structure of our discussion. Figure by author

particularly evident in risk analysis, where the absence of specific, universally accepted, objective methodologies within such standards often leaves practitioners struggling to translate high-level principles into concrete, reliable assessments. For their enduring relevance, a more scientifically grounded formulation is essential. While the precise nature of such a "scientific approach" is open to debate, any utilization of interdisciplinary insights – including those from management science – necessitates establishing a principled and systematic congruence between integrating such knowledge and its practical application. The research program discussed in this paper attempts to realize such principled and systematic congruence. It is this underlying concept that this paper proposes to term *disciplined alignment*.

2. Issues in information security management framework

This section examines critical issues within information security management, focusing initially on the fundamental misalignment in risk conceptions between managerial or business stakeholders and security practitioners. We will illustrate how this misalignment manifests in challenges such as insecure risk analysis, detachment from business risk considerations and alienation from corporate governance. Subsequently, for each of these problem areas, this section explores existing academic research and established practices from related fields – including attack graph analysis, EA and BRM – to identify potential approaches for mitigating these misalignments and fostering a more unified understanding.

2.1 Information security management framework

Several well-known standards, such as Information Security Management System (ISMS) standards (ISO/IEC, 2005a; b, 2010) and the SP-800 series, codify the information security management framework. They are based on a common conceptual model, i.e. information security management is generally regarded as a type of risk management. The ISMS standards define the core process consists of the following four steps (ISO/IEC, 2016):

(1) Risk identification: Identify risks relevant to the business.

(2) Risk analysis: Examine individual and combinatorial risks' detailed behavior and properties.

(3) Risk evaluation: Determine whether the level of risk is acceptable.

(4) Risk treatment: Take measures against unacceptable risks.

The combination of identification, analysis and evaluation is called risk assessment. The iteration of this series of steps is the common model in information security management.

The implicit assumption behind this model is that we can understand risks. Risks are supposed to be identifiable, inspectable and comparable with the predefined unacceptable level. On the other hand, risks involve some uncertainty by definition. Therefore, the model cannot be viable without somehow managing that uncertainty. If that uncertainty is handled inappropriately, risk identification, analysis and evaluation results become unreliable and the entire information security management process will be groundless.

At the same time, we must remember that information security management is an aid for smooth execution of the business, not the purpose. As with information security practices, the business requires many resources to run. General business activities and information security management compete for finite resources. If the business case for information security management is poorly supported, other business units will argue that the relevant resources should be spent on their activities.

As the situation above indicates, uncertainty handling is fundamental to information security management's viability.

2.2 Insecurity in risk analysis

2.2.1 Issues. Federal organizations are mandated to assess risks periodically (Ross *et al*., 2006) and audits shall verify their actual performance. In the OPM case, audit reports had warned of widespread non-compliance with security controls for years. Just before the incident, the semiannual internal audit report (of the Inspector General, 2013) identified "deficient security controls" in the Personnel Investigations Processing Systems (PIPS), the system with the most significant security concerns. This problem further "deteriorated" after the incident and the OPM was criticized for leaving the systems without authorizations, including risk assessment (of Audits, 2015). The OPM had opportunities to recognize the risks but prioritized usual business over security.

When business activities conflict with security concerns, a mechanism is needed to ensure security implementation. This mechanism must function even under potentially unbalanced pressure from the business side. Proper security risk analysis is an essential foundation. If risk analysis suggests substantial risk but appropriate treatment is skipped, it indicates blamable negligence. Although not an information security matter, a seismic risk analysis case preceding the Fukushima nuclear accident highlights a crucial aspect of this issue.

The Japan National Diet commission's investigation report (Fukushima Nuclear Accident Independent Investigation Commission, 2012) states that the commissioners "believe that the tsunami risk was underestimated ... Meanwhile, with regard to severe accident countermeasures, the probabilistic safety assessment of tsunamis was deemed uncertain, so the consideration itself was pushed back and measures were not taken. As such, Tokyo Electric Power Co. used probabilistic evaluations in ways that suited them in order to avoid clarifying the tsunami risk."

Risk is commonly defined as the combination of probability and impact. Underestimating probability can make risks seem insignificant. In information security, accurate statistics are often unavailable, making it easy to downplay risks by emphasizing uncertainty. Thus, risk analysis is susceptible to intentional underestimation.

Reliable information security management requires appropriately handling uncertainty and the analysis result should be robust. However, the well-known ISMS standards and SP-800 series, while organized as risk management frameworks, lack specific risk analysis methods. IEC 31010 (IEC/ISO, 2019), a reference standard, introduces 42 risk analysis methods, but most rely on analyst judgment or unavailable statistics, making it difficult for ordinary staff to obtain objective results. Similar limitations also apply to other local standards, such as ETSI CYBER (ETSI, 2017) in Europe, OCTAVE Allegro (Caralli *et al*., 2007) in the USA, IT-Grundschutz (für Sicherheit in der Informationstechnik, 2017) in Germany, EBIOS (ANSSI, 2019a, b) in France and MAGERIT (Crespo *et al*., 2006) in Spain. For example, EBIOS exemplifies a severity level table in which "long-lasting shutdown" is categorized as "critical" and "temporary shutdown" as "serious," but the distinction between them depends on analyst judgment. Also, MAGERIT elaborates on the calculation rules for risk metrics without providing necessary source statistics. None of these standards eliminate uncertainty or analyst subjectivity, leaving them open to challenge.

If the remaining uncertainty allows irresponsibly rephrasing risks as ignorable, such discretion becomes a source of abuse. At the same time, it is partly legitimate to argue that security practitioners often prefer excessive security controls (Mersinas *et al*., 2016). Viable risk analysis should arbitrate the conflict about risk conception between business and security practitioners. Since we cannot eliminate every unknown factor, such arbitration must prevent the remaining uncertainty from undermining the process.

2.2.2 Approaches. Many academic studies on information security risk metrics exist, e.g. Kordy *et al*. (2014), Ramos *et al*. (2017), Pendleton *et al*. (2017). Risk metrics enable us to compare the level of risks easily. However, we should distinguish the ease of comparison from the validity of the comparison results. Cremer *et al*. (2022) surveyed data availability and showed the shortage. Verendel (2009) points out the immaturity of the said quantitative metrics. Reliable quantitative risk metrics require that the input data are correct and that the

metrics are well-tested, but both requirements are rarely satisfiable. These weaknesses are no different from those seen in the standards mentioned above. While these two issues should be resolved in the long run, we need careful consideration when using these metrics now.

Zio (2018) discusses risk assessment's limitations and inherent characteristics and delineates it partly as a simulation of rare, critical events. The simulation represents integrated knowledge about the system and environment to be analyzed. Risk analysis based on simulated system behavior is called a model-based approach. Ramos *et al*. (2017) broadly survey model-based quantitative network security metrics. Although model-based approaches do not address the challenges posed by data and expertise shortages, they offer a valuable advantage: the ability to gain deeper insights into the mechanisms and characteristics of the risks involved. It could suggest, for instance, an effective security control to prevent the risk even when reliable statistics do not back the calculated metric. As Zio (2018) indicates, risk assessment is a means for rational decision-making and the essence of assessment is providing and extracting valuable insights for better decisions. Therefore, we can offset the inherent uncertainty in the analysis result with its practical implication; it is especially true for an approach separating uncertainty systematically from the result.

Attack graph analysis, comprehensively summarized in Zenitani (2023), is an approach worth elaborating on among past studies: a model-based approach for network security analysis generating and analyzing a directed graph called an attack graph. In one definition, it is a generalized and computerized variation of bottom-up fault tree analysis. We can obtain an attack graph from objectively identifiable information such as network topology, system configuration, distribution of vulnerabilities and known exploits. An attack graph is a consolidated depiction of logically possible attacks and the detailed steps of each attack are included there. The strength of this method is that (1) it is an algorithmic method based on objective, non-statistical data and could be suitable for implementation by non-experts and (2) it is a qualitative analysis basically, i.e. it enables security analyses separated from quantitative weighing of the result.

Phillips and Swiler (1998) proposed the first comprehensive framework of attack graph analysis. Since then, many forms of attack graphs have been examined. For example, state enumeration graphs (Jha *et al*., 2002) are a kind of finite automata. Exploit dependency graphs (Jajodia *et al*., 2005; Ou *et al*., 2006) are cyclic AND/OR graphs interpretable as a set of merged fault trees. Bayesian attack graphs (Frigault and Wang, 2008) are the recast forms of exploit dependency graphs as Bayesian networks and enable the probability calculation of malicious events if appropriate statistics are available.

We can choose the most suitable definition of attack graphs depending on data availability. In the absence of reliable data, using qualitative attack graphs like exploit dependency graphs can be a deliberate choice to avoid quantitative evaluation. In that case, we only know whether an attack is logically possible coupled with applicable security control candidates and evaluating the attack probability is delegated to additional weighing steps. Therefore, we can clarify the responsibilities of the business side, who may tend to underestimate risks, by involving them in the risk weighing and holding them accountable for their evaluations.

2.3 Distance from business risk analysis

2.3.1 Issues. Decision-makers are not interested in the server malfunctioning incident itself but in the consequential impact on the business. The security experts' knowledge is valuable for analyzing the incident effectively. The business impact, as mentioned earlier, cannot be clarified without the knowledge of business practitioners within the enterprise. Therefore, the risk assessment process requires joint efforts between the two parties, but such collaboration between people with different expertise is often challenging.

The very similar case, business-IT alignment has been a long-standing concern, with communication being a central issue. Luftman (2000) mentions the lack of mutual understanding and communication as a persistent challenge in achieving alignment.

Similarly, Vermerris *et al.* (2014) found that projects lacking effective communication mechanisms between business and IT stakeholders often resulted in misalignment and lower business value. This is echoed in Hetemi *et al.* (2022), in which the authors discuss the importance of dialogue and collaborative practices in bridging the communication gap between technical and business teams in IT projects. Their study examines the difference in styles of communication and knowledge controls between the two parties.

In the OPM case, there was a considerable gap in the perceptions between those involved in information security and business practices. For several years before the incidents occurred, the OPM's CISO and internal audit department repeatedly pointed out "material weaknesses" in information security management. In contrast, as quoted in the introduction, the OPM's operational departments were uncooperative in implementing information security measures hindering their work. Furthermore, it is noteworthy that the US Congress, which was supposed to receive the audit report, supervise and guide the OPM, was also indifferent to information security. The OPM hearings in 2009 were concerned only with processing personnel cases and no questions were raised about information security [4].

The US federal government had much guidance on risk assessment. The law and the guidance were carefully examined and information security management practices were mandated under them. Thus, the lack of such a framework was not the problem.

One possible explanation for this misalignment is the immaturity of business risk analysis methods. As discussed in the previous subsection, no objective and reliable risk analysis method is widely used. It is even more true for business risk analysis, which is broader in scope. In the OPM case, the "material weaknesses" pointed out by the audit reports were mainly about non-conformance to the security regulation and were not the direct warning about clear and recent danger. It is unclear if the nature of business risk then was shared within the OPM. At least, the audit reports to Congress did not indicate possible business impacts in detail. The insufficient business risk description could explain the malfunction of the information security management in the OPM case, in addition to the uncertainty in risk analysis.

We need a trustworthy method for business risk estimation. The method should present incontrovertible facts under a vocabulary for both sides as the basis for further discussion. Without such a method, how can security professionals convince business practitioners of the need for cumbersome security controls? Cooperative dialogue between the two parties will be deadlocked easily without its aid.

2.3.2 Approaches. EA is a method for understanding the complex relationship between IT infrastructure and business activities. Several well-known EA frameworks, such as Department of Defense Architecture Framework (DoDAF) (US Department of Defense, 2010) and Zachman Framework, have been proposed. Following these frameworks will help us describe the entire picture of an enterprise and understand the dependencies among various components, including business processes, digital services and infrastructure.

According to van den Berg *et al.* (2019), EA can significantly improve the quality of IT investment decisions by providing insights into the strategic fit of IT projects, their relationship with past and future investments and potential risks. Mavengere *et al.* (2020) highlight using EA modeling techniques to visualize and align business strategy with IT infrastructure, thus enhancing communication and collaboration between business and IT stakeholders. Niemi and Pekkola (2020) further emphasize that EA benefits extend beyond IT, influencing various organizational aspects and improving understanding and decision-making.

Enterprise Information Security Architecture (EISA) extends EA to provide a comprehensive view of security measures and their contributions. The Open Enterprise Security Architecture (O-ESA) (Wahe and Petersen, 2011) is an example of EISA, which primarily focuses on automating security monitoring and configuration management. It is now under the ownership of The Open Group but has not been updated for years. The Open Group also owns The Open Group Architecture Framework (TOGAF) (The Open Group, 2018) and

ArchiMate (The Open Group, 2019); both are the de facto standards for EA frameworks. These frameworks are not EISA, but the integration with Sherwood Applied Business Security Architecture (SABSA), an EISA proposed by Sherwood (2005) independently, has been explored (The Open Group, 2011). These efforts give us a vocabulary to depict the whole picture of an enterprise, including security measures and its relevant business activities, while not a risk analysis method.

In the literature, several risk analysis methods are proposed based on business model descriptions parallel to EA. Innerhofer-Oberperfler and Breu (2006) suggested a conceptual EA framework and proposed a top-down dependency analysis method to evaluate the impact and probability of the risk. Breu *et al*. (2008) extended this study to elaborate on an algorithm for calculating the expected loss. Zambon *et al*. (2007a, b) proposed a business availability analysis method. Johnson *et al*. (2006) have combined EA and attack tree (fault tree) analysis. In this approach, an attack tree is represented as an extended influence diagram; thus, it can calculate the probability of incidents' occurrence. Later on, Sommestad *et al*. (2008, 2009) proposed leveraging a metamodel designed with the predefined dependencies between attributes to produce the diagram. Johnson *et al*. (2013) incorporated the uncertainty in an enterprise model as probabilistic perturbation in the Monte Carlo simulation. We can regard these studies as EA-based risk analysis methods, but they are as vulnerable as the aforementioned risk analysis methods due to their dependence on reliable statistics.

Some research deals with business risk analysis as an extension of attack graph analysis. Froh and Henderson (2009) extended the inference rules used in attack graph analysis to accommodate the dependency between services and infrastructure. Johnson *et al*. (2016) proposed a threat modeling approach named "pwnpr3d," integrating the idea of EA, attack graph analysis and the Time To Compromise metric. Sun *et al*. (2017) introduced mission impact graphs as an extension to the attack graph. Cao *et al*. (2018) refined and verified the approach by Sun *et al*. (2017) and it depicts the multi-layered form of attack graph analysis parallel to EA.

The theoretical basis of exploit dependency graphs, the adopted form of attack graphs in the above studies, is logic programming based on monotonic logic. Datalog (Ceri *et al*., 1989) is a restricted logic programming language that matches this class. We can use Datalog to develop libraries for risk analysis while enjoying its powerful expressiveness (Ou *et al*., 2005). The works by Froh and Henderson (2009) and Johnson *et al*. (2016) are in line with this intuition and in fact, Johnson *et al*. (2018) have proposed a domain-specific language called Meta Attack Language (MAL); this is theoretically a variation of Datalog with additional attributes. The expressiveness of this class covers a broad range of Tactics, Techniques and Procedures (TTPs) defined in MITRE ATT&CK (Tayouri *et al*., 2023).

The prior studies mentioned above indicate that, although they could be vulnerable too in the sense mentioned previously and there is still significant room for development, a theoretical foundation for risk analysis supported by powerful expressiveness can enable various risk analyses, including business risks.

2.4 Alienation from corporate governance

2.4.1 Issues. While the content discussed above is a prerequisite for meaningful risk analysis and a necessary condition for risk management, it is insufficient. Even when risks are clear and agreed upon, stakeholders still compete for finite resources. Prioritizing information security above all else is unreasonable and decision-makers may legitimately limit risk treatments based on rational considerations. However, the line between reasonable and unbalanced restrictions can be blurry.

In the OPM case, "The Inspector General (IG) also found that the agency's Office of CIO (OCIO) lacked the authority it needed to manage security matters effectively . . . and most (of the designated security officers, DSO) are only managing their security responsibilities as a secondary duty to their primary job function . . .. the OCIO has no authority to enforce security requirements" [5].

It is easy to say that the OCIO should have been given sufficient authority in retrospect. Unfortunately, determining the appropriate level of authority before the incident is complex. Remind that security practitioners can also be biased (Mersinas *et al*., 2016). Instead, we should focus on the fact that the DSO managed its security responsibilities as secondary.

Information security is a foundation for smooth business execution and its importance never subordinates to other business requirements. The DSO should have accurately recognized the danger of operational disruption when information security is compromised. More substantial OCIO authority without ponderation would enforce compliance without addressing the underlying issue. The DSOs' conception of information security as secondary is unbalanced and is the focal misalignment that should have been addressed.

This sort of misalignment is generally exacerbated by inadequate public awareness of information security, as people tend to disregard what they need help understanding and alienate the tasks associated with those unknowns. It also applies to the members of Congress who did not raise any information security concerns during the OPM hearings. While education is crucial, we should remember that the investment of time and money for education also competes for finite resources.

Overall, we need a mechanism that naturally identifies and corrects hazardous misalignment when businesses mistakenly neglect information security efforts.

2.4.2 Approaches. Deficits in information security management practices are often attributed to governance failures, prompting calls for reinforced oversight. However, such a simplistic view overlooks the interplay between information security and business objectives, where resources are constantly competed. While immediate empowerment of information security authority might offer a short-term fix, it risks long-term misalignment.

A more sustainable approach lies in fostering a shared understanding that information security enhances corporate value. However, quantifying such contribution is demanding and controversial. This is where BRM can offer valuable insights. BRM, a structured approach not specific to information security, focuses on clarifying the contribution of technical investments, particularly in IT (Peppard *et al*., 2007). By identifying, planning and managing the delivery of benefits throughout the investment lifecycle, BRM aligns IT projects with strategic business objectives (Serra and Kunc, 2015).

A key tool within BRM is the benefits dependency network (BDN), also known as the benefits map, which visually maps the links between investment objectives, expected benefits, necessary business changes and enabling IT capabilities. This visual aid serves as a communication bridge between IT and business professionals, fostering a shared understanding without reliance on technical jargon.

PPM is another strategic approach that complements BRM. PPM manages multiple projects as a cohesive unit to achieve organizational goals (Meskendahl, 2010). It involves processes such as project selection, prioritization, resource allocation and optimization to maximize the value and strategic alignment of the project portfolio (Reyck *et al*., 2005).

When combined, BRM and PPM create a dynamic system that aligns diverse perspectives, continuously monitors ongoing projects and optimizes their mix (Thorp, 2003). This system can be highly valuable for information security management, where technical, non-technical and business elements intersect. The system enhances decision-making and consensus-building by continuously capturing and controlling deviations from presumed success.

In the face of uncertainty, achieving absolute accuracy in risk management is impossible. At the same time, inaction due to imperfect information is equally irrational. Rationality lies in the thoroughness and balance of considerations during the decision-making process. A system like BRM and PPM, which maintains a clear focus on concerns, promotes understanding among stakeholders and enables continuous alignment, is a significant step toward improved decision-making and, ultimately, better information security management.

3. Gaps between researches and practices

While the previous section introduced numerous research findings and related standards, their practical application in information security often lags. To bridge this gap and make these "tools" practically usable, certain prerequisites are missing. This is not about uncritically adopting academic outputs; research untested in practice risks remaining purely theoretical. Thus, practical validation and filling these voids are necessities that researchers should spearhead efforts to overcome. Accordingly, this section details these missing prerequisites as critical gaps including the initiatives researchers should lead to resolve them.

3.1 Lack of tools integration

The field of information security research is vast and diverse, with a wealth of findings that often remain fragmented and difficult to synthesize. Indeed, the various approaches concerning risk analysis, business alignment and governance discussed in Section 2, while individually promising, often exemplify this fragmentation when practitioners seek comprehensive, actionable solutions. While numerous advanced studies exist, few researchers, let alone practitioners, grasp the complete picture.

In practice, information security necessitates combining technical and managerial solutions, spanning risk analysis, treatment and beyond. Encouraging research findings, coupled with the challenges of integrating diverse knowledge, underscore the immense potential of combining these approaches. For instance, we can integrate attack graph analysis with an extended EA framework to conduct comprehensive business impact analyses. These results could then be merged with a BDN work and communicated to stakeholders to formulate project portfolios and guide ongoing implementation and monitoring efforts.

Ensuring the reliable performance of individual research findings in combination remains a challenge. Exploring optimal, even feasible, combinations is a complex task that demands careful consideration, as highlighted in studies by Chung *et al*. (2013), Holm *et al*. (2015), Noel *et al*. (2016). It is unrealistic to expect practitioners to navigate and integrate them independently. Given the specialized knowledge required to interpret academic literature and assess interoperability, researchers play a crucial and irreplaceable role in identifying effective integrations.

By translating research findings into employable integrations, researchers can empower practitioners to make informed decisions based on a holistic understanding of the information security management landscape and available solutions. This effort would bridge the gap between theory and practice and enhance the overall effectiveness of information security initiatives.

3.2 Lack of detailed case descriptions

While the information security research community is composed primarily of experts, the field of practice involves diverse stakeholders who may need to gain specialized knowledge in information security. Even if optimal integrations of research findings are identified, their effectiveness hinges on their accessibility and comprehensibility to practitioners.

Developing user-friendly tools and resources that effectively communicate research results to a broader audience is crucial. This includes creating guidance materials tailored for non-experts and developing educational resources to support training initiatives. Li *et al*. (2019) found that organizational efforts to enhance cybersecurity awareness and provide training significantly influence employees' cybersecurity behaviors. These efforts should be a collaborative endeavor between researchers and practitioners.

However, as evidenced by the OPM data breach, the mere availability of guidance does not guarantee the successful implementation of information security management. Implementing well-researched and organized methods requires additional steps beyond providing guidance materials (AlGhamdi *et al*., 2020). These steps may involve addressing the cognitive and

affective factors influencing employee compliance behavior (D'Arcy and Lowry, 2019; Bulgurcu *et al*., 2010).

Management standards, particularly in domains like information security, are often described abstractly to ensure broad applicability across diverse organizations. This inherent generality frequently poses challenges when practitioners attempt to translate these high-level principles into concrete actions tailored to their specific operational realities (Culot *et al*., 2021; Diesch *et al*., 2020). Such implementation difficulties can be exacerbated when attempting to fuse or harmonize standards from disparate management domains, such as information security management and BRM, a process which can lead to confusion and ineffective implementation due to overlapping efforts and structural differences between models. The integration of various standards, for instance, can present substantial issues related to differing scopes, requirements, partial overlaps and terminology (Wangenheim *et al*., 2010). Managerial best practices often rely on tacit knowledge and experience, resembling an art rather than a science.

Researchers can contribute by providing practitioners with a rich repository of detailed case descriptions that illustrate the application of abstract management standards to specific contexts could significantly aid practical implementation, as the current lack of precise methodological indications can translate into inaccuracies and an easy-to-understand toolkit is often missing. At a minimum, failing to offer such elaborated examples and instead assigning the responsibility of detailed concretization solely to practitioners – who may not always be fully competent with the underlying concepts of the standards – risks leading to significant practical difficulties and a fallback to *ad-hoc* implementations.

3.3 Lack of performance validation

Information security is a practical science, seeking solutions within a changing societal landscape rather than pursuing eternal truths. Actual practices must validate the value of studies in this field. Nevertheless, the sensitive nature of information security prevents organizations from openly sharing details about incidents, practices and even policies. The unavailability of public data identified by Cremer *et al*. (2022) reflects this constraint. This lack of transparency constrains most security studies to lack practice-based validation and depend on conceptual elaboration and numerical experiments. Limited communication between researchers and practitioners impedes advancements and creates a disconnect between research and practice.

From a practitioner's perspective, this lack of validation introduces uncertainty into their work. When perceived security levels are insufficient, the root cause could lie in implementing standardized best practices or in the design of those practices themselves. Distinguishing between these two is crucial, as the latter necessitates tailoring. It is easier said than done, as understanding the nuances of best practices requires specialized expertise that only some practitioners possess. The DSOs in the OPM case exemplify this issue, as they were chosen among non-security professionals.

Researchers can address this challenge by developing accessible validation benchmarks that incorporate the latest research findings and providing guidance on their interpretation and use in different contexts. Such benchmarks could provide practitioners with a clearer understanding of the expected outcomes of implementing best practices, facilitating the identification of implementation issues and the need for specific tailoring.

4. A proposal of a research program

The hand-in-hand relationship between researchers and practitioners is the basis of sound information security management research and practice. Here, we try to clarify what researchers can do to build mutual trust. It is a research program devoted to establishing a concrete and robust foundation for fulfilling the aforementioned three gaps.

4.1 Make employable integrations

The initial step is to define and elaborate on how to integrate state-of-the-art research findings in the field of information security into actionable solutions for practitioners. To address the fragmentation of tools and methodologies highlighted in Section 3.1—particularly concerning the array of approaches introduced in Section 2 – this initial step of the research program focuses on establishing a framework for their employable integration. This framework organizes, from a perspective of logical consistency, the interrelationships among the approaches mentioned in Section 2.2 to Section 2.4, ensuring they function effectively when applied to the corresponding issues. The following three tiers are structured accordingly, each corresponding to one of these respective sections:

(1) *Foundational theory of secured risk analysis:* The first tier should establish a rigorous mathematical foundation for categorizing risk descriptions based on their robustness against intentional undervaluation. Separating qualitative analysis from quantitative evaluation could serve as a potential starting point and attack graph analysis is a candidate for further development.

(2) *Library and techniques for business risk analysis:* Building upon the mathematical foundation of the first tier, the second tier should enable comprehensive business risk analysis leveraging the robustness established in the previous tier. Business risks encompass a broader vocabulary than simple security incident analysis, necessitating a library of clearly defined relevant elements. This tier should also incorporate business risk analysis algorithms coupled with this library.

(3) *Concrete process model focusing on consensus-building with explicitly stated grounds:* The business risk analysis mentioned above enables discussions among stakeholders in a manner more relevant to the actual value of their business. Still, inherent uncertainties necessitate a focus on consensus-building rather than relying solely on systematic procedures. The consensus-building process should meticulously document the premises and referenced information used in decision-making for future reference and audits. This tier provides a management process model that leverages the robust business risk analysis method defined in the base tiers while securing the preservation of decision inputs. This process model does not immediately imply validation but provides a foundation for enabling objective validation.

Researchers can independently initiate the development of various integrated methodologies based on the three tiers outlined above. The resulting deliverable would be a suite of carefully chosen techniques encompassing the full spectrum of information security management. This comprehensive resource would be a foundation for further communication and collaboration between researchers and practitioners.

4.2 Provide imaginary case descriptions

As Section 3.2 elaborates, a key element of this research program involves developing and disseminating practical and detailed case descriptions. Given that real-world examples fully embody the integrated methodology proposed herein, such cases will likely emerge only as the research program matures and the initial creation of illustrative hypothetical scenarios is considered essential. These meticulously constructed cases depicting varied security landscapes and management challenges can serve as valuable “living textbooks” for practitioners seeking to translate abstract concepts into their specific operational contexts.

A significant advantage of these hypothetical case studies is their independence from the disclosure sensitivities often associated with real-world corporate security information. This characteristic permits the research community to openly share, rigorously analyze and iteratively refine them. Consequently, such detailed imaginary scenarios can function

effectively as reference testbeds, facilitating the testing, validation and further development of the methodologies and tools advanced within this research program.

4.3 Clarify the verification and validation criteria

The proposed integration is just a hypothesis and we need to test it repeatedly and refine it gradually. This iterative improvement is a joint effort of researchers and practitioners. Both parties have their responsibility and role in accomplishing the contribution. Therefore, it is of critical importance to have criteria that verify and validate the implementation of each party's effort.

Verification criteria examine the practitioners' implementation of the integrated methodology. It corresponds to the gap in Section 3.3 and should focus on the factors affecting the successful performance, including, for instance, governance structure, internal compliance in the handling of risk register, accuracy and exhaustiveness of configuration management and level of general risk awareness among an enterprise.

Validation criteria provide multi-faceted viewpoints for the definition of successful implementation of information security management. The key question behind the evaluation should be the alignment with the ideal concept and the business value—the former alignment tests practitioners' level of understanding of the articulated methodology. In contrast, the latter alignment implies that any information security management practice is justified when and only when it contributes to the business value.

While clarifying these criteria requires substantial research, existing studies and best practices can serve as a starting point. These are not novel concepts. It is legitimate to find a similarity with the Verification and Validation model (Hirshorn *et al*., 2017). Within the proposed research program, the criteria have a specific role in facilitating communication and mutual trust between researchers and practitioners. Therefore, these criteria should be framed as suggestions rather than rigid constraints, functioning as a protocol to reduce miscommunication and foster collaboration.

4.4 Hypothetical proof of concept

Here, we present a blend of past studies and best practices as an implemented case of the proposed research program. It is not a recommendation but an experimental suggestion that might work in practice. It is an imaginary best practice of disciplined alignment. This subsection clarifies how the components discussed above work together.

We outline the practical application of the proposed three tiers, showcasing their potential relevance and feasibility.

(1) *Foundational theory of secured risk analysis:* Utilize attack graph analysis with exploit dependency graphs, ensuring a clear separation of qualitative analysis from quantitative evaluation. This is inherent to the mathematical nature of exploit dependency graphs. Moreover, multi-resolution attack graph analysis (Zenitani, 2022) provides a mechanism robust against risk underestimation, as fewer investments in analysis inherently overestimate risk scenarios.

(2) *Library and techniques for business risk analysis:* Attack graph analysis is essentially a logic programming process, where each risk analysis becomes the development of a risk analysis program. Languages like MAL (Johnson *et al*., 2018) or Datalog can be used for this purpose. EA frameworks (e.g. TOGAF, ArchiMate) provide a core vocabulary for describing the enterprise, while security-specific vocabulary can be drawn from past studies (Ou *et al*., 2005; Tayouri *et al*., 2023). The integration of enterprise and security descriptions has been well-documented in previous research (Froh and Henderson, 2009; Sun *et al*., 2017; Cao *et al*., 2018). The tool "pwnPr3d," developed by Johnson *et al*. (2016), is a working example of such integration.

(3) *Concrete process model focusing on consensus-building with explicitly stated grounds:* The tools from the first two tiers enable qualitative and quantitative risk assessment. Quantitative evaluation requires acceptance of potentially incomplete statistics, necessitating an authorization process. Integrate this process with the definition of outcome/benefit measurement in BRM. Combining PPM with attack graph analysis and enhanced BRM formalizes the information security governance process. This clarifies accountability for risk assessment and facilitates communication between security practitioners and business stakeholders, aided by BDN. Antunes and Guerreiro (2020) also discuss using ArchiMate to incorporate BDN. The entire process should be digitally recorded for post-audits and learning.

In addition to the above three tiers integration, a public repository hosting vocabulary from the second tier can also serve as a library of imaginary cases, depicting EISAs of hypothetical enterprises. These cases provide templates for practitioners and enable researchers to conduct numerical experiments for metrics development, algorithm research and design pattern exploration.

The verification and validation criteria are given as a part of the handbook explaining the usage of the above three tiers of deliverables. Regarding criteria, it is better to have an online observatory to continuously gather information about the verification and validation benchmarking results among practitioners. It enables researchers to identify the problems in the designed system and practitioners to quickly comprehend their conformance level or maturity to the best practice.

The description above is not a definitive solution, but a potential path forward. The theoretical tools are available, but further academic scrutiny and debate are necessary to fully realize the working mechanism.

4.5 Toward a disciplined alignment

Let us review what we have discussed up to here. Firstly, we have put our attention on the OPM case. It depicted the catastrophic failure of information security management. Subsequently, we have enumerated the issues in information security management and the researchers' efforts to tackle those issues. The main concern was the misaligned conception of information security between security practitioners and business staff. Then, we have examined further the gaps between information security researchers and practitioners. The gaps impede positive collaboration in continuously advancing research and practice. Lastly, we have proposed a draft of a research program to reconcile those misalignments.

The focus is on the misalignment between security practitioners and business staff and that between researchers and practitioners. At the very beginning, we must accept that we cannot eliminate all the uncertainties. We can only behave, at best, rationally to cope with the inherent uncertainty in the world. At the same time, every person struggles to thrive and has the right to choose one's action based on their standpoint, which is rational behavior. The failure in management is often a by-product of conflicts among those different rationalities. Integrating each stakeholder's perspective in a way overcoming the conflicts shall contribute to the organizational mission at its best performance.

The alignment in stakeholders' conceptions and behaviors is the foundation of the best risk management and should be scientifically disciplined if we want to replicate it everywhere in need. Such an attempt to make a new discipline requires the definition of alignment and evaluation criteria for the level of alignment, the process model for consensus-building and the method for explicit and objective descriptions of decision-making materials. The combination of making employable integration of existing studies and defining verification and validation criteria is a starting point of this research. It is a mixture of science and practice, enables further collaboration between researchers and practitioners and facilitates cooperation between business and security practitioners towards a *disciplined alignment*.

5. Limitations

This article is presented as a concept paper, aiming to stimulate discussion by proposing an initial framework for disciplined alignment in information security management and a corresponding research program to develop this notion further. As introduced herein, the concept represents a foundational proposal rather than a fully matured theory. While this paper outlines its essential components and intended direction, the proposed framework's precise definition, scope and operationalization warrant ongoing academic discourse and refinement through practical application.

As a concept paper, this article does not report empirically validated research findings. Rather, it represents an organized articulation of the author's critical perspectives and awareness of the issues, structured primarily to invite further discussion and debate. Consistent with this conceptual nature, the gaps between research and practice identified in Section 3 are based on the author's experience and a broad review of existing literature rather than a systematic empirical investigation or a formalized literature review protocol. Consequently, the list of gaps presented does not intend to be exhaustive and other significant impediments to the practical application of research findings in practice may exist. The primary purpose of identifying these gaps was to highlight critical areas the proposed research program could contribute to developing the aforementioned guiding principle. Future empirical research is beneficial to further validate, refine and expand upon the gaps discussed herein, which inform its ongoing development.

Similarly, the practical feasibility, effectiveness and potential challenges of implementing the proposed three-tiered integration and the associated processes – and its further articulation – will require substantial future study. The research program intends to lay a foundation and provide a structured direction for such endeavors rather than presenting a complete, validated solution or a finalized theoretical construct.

6. Conclusion

This article refers to the OPM data breach to discuss the issues in the information security management concept. We pointed out three issues: vulnerability to intentional sophism in information security risk analysis, immaturity in business risk analysis methods and the tendency of information security decoupling from corporate governance. These reflect the misalignment between security and business practitioners' conceptions. Although information security researchers have made several approaches to these challenges, there is plenty of room for further development. There are also gaps between researchers and practitioners that inhibit the productive collaboration of the two parties. Those gaps are the lack of employable integration of existing studies, the lack of detailed case descriptions and the lack of verification and validation criteria with the communication process of actual cases. A draft research program is proposed to overcome these issues and build mutual trust among researchers and practitioners. It urges the employable integration of existing studies and clarifies the verification and validation criteria for practices to facilitate the reconciliation of risk misconceptions between business and security practitioners. All these efforts shall contribute to the broader collaboration toward the disciplined alignment of managerial activities.

Acknowledgments

The author wishes to acknowledge Dr Keisuke Tanaka, Professor in the Department of Mathematical and Computing Science, School of Computing, Tokyo Institute of Technology, for reviewing and providing constructive advice on the drafts of this article. Several AI tools, including Google Gemini, Grammarly and DeepL, have assisted in writing this article.

Notes

1. Committee on Oversight and Government Reform (2016, p. iii).
2. Committee on Oversight and Government Reform (2016, p. 38).

3. Committee on Oversight and Government Reform (2016, p. 76).
4. Committee on Oversight and Government Reform (2016, p. 39).
5. Committee on Oversight and Government Reform (2016, pp. 40–41).

References

AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E. (2020), "Information security governance challenges and critical success factors: systematic review", *Computers and Security*, Vol. 99, 102030, doi: 10.1016/j.cose.2020.102030.

ANSSI (2019a), "Ebios risk manager", available at: https://cyber.gouv.fr/publications/ebios-risk-manager-method

ANSSI (2019b), "Ebios risk manager: going further", available at: https://cyber.gouv.fr/sites/default/files/2019/11/anssi-guide-ebios_risk_manager-going_further-en-v1.0.pdf

Antunes, F. and Guerreiro, S. (2020), "Integrating benefits dependency network in archimate".

Breu, R., Innerhofer-Oberperfler, F. and Yautsiukhin, A. (2008), "Quantitative assessment of enterprise security system", *2008 Third International Conference on Availability, Reliability and Security (ARES'08)*, pp. 921-928, doi: 10.1109/ARES.2008.164.

Bulgurcu, C., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, p. 523, doi: 10.2307/25750690, available at: https://www.jstor.org/stable/10.2307/25750690

Cao, C., Yuan, L.P., Singhal, A., Liu, P., Sun, X. and Zhu, S. (2018), "Assessing attack impact on business processes by interconnecting attack graphs and entity dependency graphs", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 330-348, 10980 LNCS, doi: 10.1007/978-3-319-95729-6_21.

Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R. (2007), "Introducing octave allegro: improving the information security risk assessment process".

Ceri, S., Gottlob, G. and Tanca, L. (1989), "What you always wanted to know about Datalog (and never dared to ask)", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 1 No. 1, pp. 146-166, doi: 10.1109/69.43410.

Chung, C.J., Khatkar, P., Xing, T., Lee, J. and Huang, D. (2013), "NICE: network intrusion detection and countermeasure selection in virtual network systems", *IEEE Transactions on Dependable and Secure Computing*, Vol. 10 No. 4, pp. 198-211, doi: 10.1109/TDSC.2013.8.

Committee on Oversight and Government Reform (2016), "The OPM data breach: how the government jeopardized our national security for more than a generation", Technical Report, U.S. House of Representatives.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S. (2022), "Cyber risk and cybersecurity: a systematic review of data availability", *Geneva Papers on Risk and Insurance: Issues and Practice*, Vol. 47 No. 3, pp. 698-736, doi: 10.1057/s41288-022-00266-6.

Crespo, F.L., Angel, M., Gómez, A., Centro, J.C., Nacional, C. and Nas, J.A.M. (2006), "Magerit-version 2 methodology for information systems risk analysis and management iii-techniques project team", available at: http://publicaciones.administracion.es

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *TQM Journal*, Vol. 33 No. 7, pp. 76-105, doi: 10.1108/tqm-09-2020-0202.

Diesch, R., Pfaff, M. and Krcmar, H. (2020), "A comprehensive model of information security factors for decision-makers", *Computers and Security*, Vol. 92, 101747, doi: 10.1016/j.cose.2020.101747.

D'Arcy, J. and Lowry, P.B. (2019), "Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study", *Information Systems Journal*, Vol. 29 No. 1, pp. 43-69, doi: 10.1111/isj.12173.

ETSI (2017), "Ts 102 165-1 – v5.2.3 – cyber; methods and protocols; part 1: method and pro forma for threat, vulnerability, risk analysis (tvra)", available at: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

Frigault, M. and Wang, L. (2008), "Measuring network security using Bayesian network-based attack graphs", *2008 32nd Annual IEEE International Computer Software and Applications Conference*, IEEE, pp. 698-703, doi: 10.1109/COMPSAC.2008.88.

Froh, M. and Henderson, G. (2009), *MulVAL Extensions II, Technical Report DRDC Ottawa CR 2009-132*, Defence R&D Canada, Ottawa.

Fukushima Nuclear Accident Independent Investigation Commission (2012), "The official report of the Fukushima nuclear accident independent investigation commission", Technical Report, The National Diet of Japan, available at: http://www.nirs.org/fukushima/naiic_report.pdf

für Sicherheit in der Informationstechnik, B. (2017), "Bsi-standard 200-3 - risk analysis based on it-grundschutz", available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Hetemi, E., Pushkina, O. and Zerjav, V. (2022), "Collaborative practices of knowledge work in it projects", *International Journal of Project Management*, Vol. 40 No. 8, pp. 906-920, doi: 10.1016/j.ijproman.2022.10.004.

Hirshorn, S.R., Voss, L.D. and Bromley, L.K. (2017), "Nasa systems engineering handbook", Technical report.

Holm, H., Shahzad, K., Buschle, M. and Ekstedt, M. (2015), "P2CySeMoL: predictive, probabilistic cyber security modeling language", *IEEE Transactions on Dependable and Secure Computing*, Vol. 12 No. 6, pp. 626-639, doi: 10.1109/tdsc.2014.2382574.

IEC/ISO (2019), "IEC 31010:2019 risk management – risk assessment techniques".

Innerhofer-Oberperfler, F. and Breu, R. (2006), "Using an enterprise architecture for IT risk management", *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, pp. 1-12, doi: 10.1.1.108.6754.

Investigation Committee on Information Leakage due to Unauthorized Access (2015), "Report on the results of the investigation into the incident of information leakage due to unauthorized access", Technical report, Japan Pension Service, available at: https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.files/press0820.pdf

ISO/IEC (2005a), "Information technology – security techniques – code of practice for information security management".

ISO/IEC (2005b), "Information technology – security techniques – information security management systems – requirements".

ISO/IEC (2010), "Information technology – security techniques – information security management system implementation guidance".

ISO/IEC (2016), "Information technology – security techniques – information security management systems – overview and vocabulary".

Jajodia, S., Noel, S. and O'Berry, B. (2005), "Topological analysis of network attack vulnerability", in *Managing Cyber Threats*, Springer-Verlag, New York, pp. 247-266, doi: 10.1007/0-387-24230-9_9.

Jha, S., Sheyner, O. and Wing, J. (2002), "Two formal analysis of attack graphs", *Proceedings – Computer Security Foundations Workshop, 15th IEEE*, pp. 49-63, doi: 10.3724/SP.J.1001.2010.03584.

Johnson, P., Lagerström, R., Närman, P. and Simonsson, M. (2006), "Extended influence diagrams for enterprise architecture analysis", *2006 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06)*, pp. 3-12, doi: 10.1109/EDOC.2006.27.

Johnson, P., Ullberg, J., Buschle, M., Franke, U. and Khurram, S. (2013), "P2AMF: predictive, probabilistic architecture modeling framework", *Enterprise Interoperability – Proceedings of the Fifth International IFIP Working Conference, IWEI 2013*, pp. 104-117, doi: 10.1007/978-3-642-36796-0.

Johnson, P., Vernotte, A., Ekstedt, M. and Lagerström, R. (2016), "pwnPr3d: an attack-graph-driven probabilistic threat-modeling approach", *Proceedings – 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pp. 278-283, doi: 10.1109/ARES.2016.77.

Johnson, P., Lagerström, R. and Ekstedt, M. (2018), "A meta language for threat modeling and attack simulations", *ACM International Conference Proceeding Series*, pp. 1-8, doi: 10.1145/3230833.3232799.

Kordy, B., Piètre-Cambacédès, L. and Schweitzer, P. (2014), "DAG-based attack and defense modeling: don't miss the forest for the attack trees", *Computer Science Review*, Vols 13-14, pp. 1-38, doi: 10.1016/j.cosrev.2014.07.001.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Luftman, J. (2000), "Assessing business-it alignment maturity", *Communications of the Association for Information Systems*, Vol. 4, doi: 10.17705/1cais.00414.

Mavengere, N.B., Pekkola, S. and Stefanidis, A. (2020), "Business-it alignment: the struggle continues", Vol. 25.

Mersinas, K., Hartig, B., Martin, K.M. and Seltzer, A. (2016), "Are information security professionals expected value maximizers?: an experiment and survey-based test", *Journal of Cybersecurity*, Vol. 2 No. 1, pp. 57-70, doi: 10.1093/cybsec/tyw009.

Meskendahl, S. (2010), "The influence of business strategy on project portfolio management and its success – a conceptual framework", *International Journal of Project Management*, Vol. 28 No. 8, pp. 807-817, doi: 10.1016/j.ijproman.2010.06.007.

National Center of Incident Readiness and Strategy for Cybersecurity (2015), "Results of the investigation into the cause of the personal information leak at the Japan Pension Service", Technical report, Cybersecurity Strategic Headquarters, available at: https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

Niemi, E. and Pekkola, S. (2020), "The benefits of enterprise architecture in organizational transformation", *Business and Information Systems Engineering*, Vol. 62 No. 6, pp. 585-597, doi: 10.1007/s12599-019-00605-3.

NIST (2008), "Performance measurement guide for information security", Technical Report July, National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.SP.800-55r1.

NIST (2011), "Managing information security risk: organization, mission, and information system view", Technical Report March, National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.SP.800-39.

NIST (2012), "Guide for conducting risk assessments", doi: 10.6028/NIST.SP.800-30r1.

NIST (2013), "Security and privacy controls for federal information systems and organizations", Technical Report September 2020, National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.SP.800-53r4.

NIST (2014), "Assessing security and privacy controls in federal information systems and organizations", Technical Report December 2014, National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.SP.800-53Ar4.

NIST (2018), "Risk management framework for information systems and organizations", Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, doi: 10.6028/NIST.SP.800-37r2.

Noel, S., Harley, E., Tam, K.H., Limiero, M. and Share, M. (2016), *CyGraph: Graph-Based Analytics and Visualization for Cybersecurity*, 1st ed., Vol. 35, Elsevier B.V., doi: 10.1016/bs.host.2016.07.001.

of Audits, O. (2015), "4a-ci-00-15-011, final audit report, federal information security modernization act audit fy 2015".

of the Inspector General, O. (2013), "Sar49, semiannual report to congress, April 1, 2013 through September 30, 2013".

Ou, X., Govindavajhala, S. and Appel, A.W. (2005), "MulVAL: a logic-based network security analyzer", *Proceedings of the 14th Conference on USENIX Security Symposium*, Vol. 14, available at: https://www.usenix.org/conference/14th-usenix-security-symposium/mulval-logic-based-network-security-analyzer

Ou, X., Boyer, W.F. and McQueen, M.A. (2006), "A scalable approach to attack graph generation", *Proceedings of the 13th ACM Conference on Computer and Communications Security – CCS'06*, ACM Press, New York, NY, pp. 336-345, doi: 10.1145/1180405.1180446.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H. and Xu, S. (2017), "A survey on systems security metrics", *ACM Computing Surveys*, Vol. 49 No. 4, pp. 1-35, doi: 10.1145/3005714.

Peppard, J., Ward, J. and Daniel, E. (2007), "Managing the realization of business benefits from it investments", *MIS Quarterly Executive*, Vol. 6, p. 1.

Phillips, C. and Swiler, L.P. (1998), "A graph-based system for network-vulnerability analysis", *Proceedings of the 1998 Workshop on New Security Paradigms*, pp. 71-79, doi: 10.1145/310889.310919.

Ramos, A., Lazar, M., Filho, R.H. and Rodrigues, J.J.P.C. (2017), "Model-based quantitative network security metrics: a survey", *IEEE Communications Surveys and Tutorials*, Vol. 19 No. 4, pp. 2704-2734, doi: 10.1109/COMST.2017.2745505.

Reyck, B.D., Grushka-Cockayne, Y., Lockett, M., Calderini, S.R., Moura, M. and Sloper, A. (2005), "The impact of project portfolio management on information technology projects", *International Journal of Project Management*, Vol. 23 No. 7, pp. 524-537, doi: 10.1016/j.ijproman.2005.02.003.

Ross, R., Katzke, S. and Johnson, L. (2006), "Minimum security requirements for federal information and information systems".

Serra, C.E.M. and Kunc, M. (2015), "Benefits realisation management and its influence on project success and on the execution of business strategies", *International Journal of Project Management*, Vol. 33 No. 1, pp. 53-66, doi: 10.1016/j.ijproman.2014.03.011.

Sherwood, N.A. (2005), *Enterprise Security Architecture: A Business-Driven Approach*, CRC Press, Boca Raton.

Sommestad, T., Ekstedt, M. and Johnson, P. (2008), "Combining defense graphs and enterprise architecture models for security analysis", *Proceedings – 12th IEEE International Enterprise Distributed Object Computing Conference (EDOC'08)*, pp. 349-355, doi: 10.1109/EDOC.2008.37.

Sommestad, T., Ekstedt, M. and Johnson, P. (2009), "Cyber security risks assessment with bayesian defense graphs and architectural models", *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences (HICSS)*, pp. 1-10, doi: 10.1109/HICSS.2009.141.

Sun, X., Singhal, A. and Liu, P. (2017), *Towards Actionable Mission Impact Assessment in the Context of Cloud Computing*, Springer International Publishing, pp. 259-274, available at: https://link.springer.com/10.1007/978-3-319-61176-1http://www.mendeley.com/research/lecture-notes-computer-science-2/

Tayouri, D., Baum, N., Shabtai, A. and Puzis, R. (2023), "A survey of mulval extensions and their attack scenarios coverage", *IEEE Access*, Vol. 11, pp. 27974-27991, doi: 10.1109/access.2023.3257721.

The Open Group (2011), "TOGAF® and SABSA® integration", available at: https://publications.opengroup.org/w117

The Open Group (2018), "The TOGAF® standard", Version 9.2, Van Haren Publishing, available at: https://pubs.opengroup.org/architecture/togaf9-doc/arch/

The Open Group (2019), *ArchiMate® 3.1 Specification*, Van Haren Publishing, Zaltbommel.

Thorp, J. (2003), *The Information Paradox: Realizing the Business Benefits of Information Technology*, McGraw-Hill Ryerson, Toronto.

US Department of Defense (2010), "The DoDAF architecture framework version 2.02".

van den Berg, M., Slot, R., van Steenbergen, M., Faasse, P. and vanÂ Vliet, H. (2019), "How enterprise architecture improves the quality of it investment decisions", *Journal of Systems and Software*, Vol. 152, pp. 134-150, doi: 10.1016/j.jss.2019.02.053.

Verendel, V. (2009), "Quantified security is a weak hypothesis", *Proceedings of the 2009 Workshop on New Security Paradigms Workshop – NSPW'09*, ACM Press, New York, NY, p. 37, doi: 10.1145/1719030.1719036.

Verification Committee for the Incident of Information Leakage due to Unauthorized Access at Japan Pension Service (2015), "Verification report", Technical Report, Ministry of Health, Labour and Welfare, available at: https://www.mhlw.go.jp/stf/shingi2/0000095311.html

Vermerris, A., Mocker, M. and Heck, E.V. (2014), "No time to waste: the role of timing and complementarity of alignment practices in creating business value in it projects", *European Journal of Information Systems*, Vol. 23 No. 6, pp. 629-654, doi: 10.1057/ejis.2013.11.

Wahe, S. and Petersen, G. (2011), *Open Enterprise Security Architecture (O-ESA): A Framework and Template for Policy-Driven Security*, Van Haren Publishing, Zaltbommel.

Wangenheim, C.G.V., Silva, D.A.D., Buglione, L., Scheidt, R. and Prikladnicki, R. (2010), "Best practice fusion of cmmi-dev v1.2 (pp, pmc, sam) and pmbok 2008", *Information and Software Technology*, Vol. 52 No. 7, pp. 749-757, doi: 10.1016/j.infsof.2010.03.008.

Zambon, E., Bolzoni, D., Etalle, S. and Salvato, M. (2007a), "A model supporting business continuity auditing and planning in information systems", *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, p. 33, doi: 10.1109/ICIMP.2007.4.

Zambon, E., Bolzoni, D., Etalle, S. and Salvato, M. (2007b), "Model-based mitigation of availability risks", in *Second IEEE/IFIP International Workshop on Business-Driven IT Management (BDIM'07)*, pp. 75-83, doi: 10.1109/BDIM.2007.375014.

Zenitani, K. (2022), "A formal approach for secured risk analysis in information security management", *IEEE*, pp. 1-7, doi: 10.1109/besc57393.2022.9995464, available at: https://ieeexplore.ieee.org/document/9995464/

Zenitani, K. (2023), "Attack graph analysis: an explanatory guide", *Computers and Security*, Vol. 126, 103081, doi: 10.1016/j.cose.2022.103081, available at: https://linkinghub.elsevier.com/retrieve/pii/S0167404822004734

Zio, E. (2018), "The future of risk assessment", *Reliability Engineering and System Safety*, Vol. 177, pp. 176-190.

Corresponding author
Kengo Zenitani can be contacted at: k_zenitani@phd.jpn.org