A picture containing text, display

Description automatically generated

Your next threat is analogue.

Enhancing security through

standardisation & digitalisation

# **Abstract**

Traditional programmatic approaches need the ability to manage controls dynamically in the complex and dynamic security threat landscape. Digital solutions are increasingly seen as vital tools and must be enabled by solid standard security risk assessment processes.

**Paul Mercer MPhil CSyP** **SyI**: [paul@hssrm.com](mailto:paul@hssrm.com)

Text

Description automatically generatedLogo

Description automatically generated

*Managing risk is challenging and taking effective action can be overwhelming.*

*HawkSight specialises in making Security Risk Management simple.*

*We give our clients simple and effective solutions enabling the creation of a safe and positive working culture that supports business growth.*

*By working closely with our clients to understand their unique business requirements, we provide tailored solutions for Enterprise Security Risk Management.*

*We term it software with a service.*

*We believe effective decision-making is driven by risk-led conversation throughout the enterprise, informing action to address uncertain outcomes.*

Reliable data and precise insight support effective risk management, enhances employee safety and drives business opportunity and growth.

Table of Contents

[Abstract 1](file:////Users/paulmercer/Library/CloudStorage/OneDrive-SharedLibraries-HawkSight/Marketing%20-%20Documents/Campaigns/Your%20next%20threat%20is%20analogue.v2.0.200623.docx#_Toc138238777)

[Introduction 4](#_Toc138238778)

[The Challenges Faced by Modern Security Professionals 5](#_Toc138238779)

[Time to get ahead of the Threat! 6](#_Toc138238780)

[Why is Standardising Your SRM Process Beneficial? 7](#_Toc138238781)

[What Does Digitalisation Mean? 9](#_Toc138238782)

[What are the Advantages of Digitalising Your SRM Process? 11](#_Toc138238783)

[Significant Time Efficiency 11](#_Toc138238784)

[Standardisation 11](#_Toc138238785)

[Compliance 12](#_Toc138238786)

[Communication 12](#_Toc138238787)

[Holistic security management 13](#_Toc138238788)

[Continuity 14](#_Toc138238789)

[Digital SRM Compatibility with ERM 14](#_Toc138238790)

[Answering the Challenges of Modern Security Professionals 16](#_Toc138238791)

[Summary 17](#_Toc138238792)

[About the Author 18](#_Toc138238793)

# Introduction

This white paper examines the intricate and ever-changing landscape of security, asserting that conventional security management techniques fall short in their ability to adapt and enforce adequate control measures dynamically.

**The imperative is clear: a progressive, forward-looking approach**

**to security is vital.**

Drawing upon real experiences, the paper illustrates the complexities of security management using an episode that transpired during an election monitoring mission in Ethiopia to demonstrate the value of effective risk analysis. An accidental shooting by security forces caused disorder at a crucial election site, and the ensuing threat of a revenge attack placed the stationed election observers at substantial risk. This incident highlights the urgent need for a systematic and rational approach to threat evaluation, particularly in situations where direct intelligence is scarce.

The threat assessment was conducted using a standardised process, leading to the decision to evacuate the observers. Although disruptive to the mission, this choice was later validated by the subsequent explosion at the election site. This intense, high-risk circumstance serves as a strong testament to effective risk communication, evaluation, and decision-making.

Yet, at a corporate level, assessing the global threat landscape and disseminating potential risks across the organisation presents a formidable challenge. This task surpasses the cognitive capacity of security professionals, and manual risk evaluations can't keep up with threats' swift emergence and mutation.

The foundation of effective security management lies in creating and maintaining an accurate enterprise-level security risk profile. Manual methods are labour-intensive, prone to errors and require extensive data analysis. To address this, the paper recommends a systematic, digital approach that ensures accuracy and accountability, improving efficiency and decreasing demand for human resources.

The ultimate goal is to empower business leaders to make real-time, informed decisions, bolstered by a resilient and dynamic security management approach. This will substantiate the worth of security by promoting business growth and maintaining a safer business environment.

# The Challenges Faced by Modern Security Professionals

In a series of interviews by HawkSight with international security professionals, it was intended to gain a comprehensive understanding of the unique challenges they face within the continually evolving business environment. Here is a summary of our findings:

|  |  |
| --- | --- |
|  | **Consensus**  Global organisations must establish a unified agreement on the most efficient strategies for handling both physical and digital security matters. |
|  | **Staffing**  Due to economic limitations, the scale of security teams has been reduced. Concurrently, these teams are tasked with addressing increasingly intricate challenges, including those beyond the traditional scope of security, such as responses to global health crises. |
|  | **Financial Constraints**  Considerable budget constraints are hindering the security department's capacity to achieve current Key Performance Indicators (KPIs) and to implement a security strategy grounded in risk management processes aligned with the broader business. |
|  | **Standardisation**  The absence of a standardized security risk management approach comprehensible to the broader business has led to a disconnect between the security team and other business units. Even within security teams, there is a reported lack of a shared understanding regarding threats and risks, indicating the need for additional training. |
|  | **Compliance**  Security leaders often rely on a compliance-centric approach that diminishes the annual security risk assessments to mere routine verifications. This methodology undermines the strategic significance of these evaluations and the potential value that the security department can contribute. |
|  | **Communication**  The lack of effective communication between the security department and the broader organization is intensified due to the absence of standardized security risk reporting and misalignment with primary business goals. This situation further hampers the potential contributions that the security department can provide. |
|  | **Governance**  Many security management strategies do not align well with the central business processes, resulting in weak governance and a noticeable disconnection from business leadership. |

# Time to get ahead of the Threat!

Traditional security models have often been entrenched in a programmatic compliance framework, fostering a perception of the security function as merely a cost center rather than a value-adding component.

Security management strategies steeped purely in compliance tend to concentrate on auditing pre-established control measures without challenging their ongoing relevance and effectiveness in the face of evolving threats. In the UK, a recent assessment of some Standard Operating Procedures of third-party security providers showed that these counter-terrorist measures were primarily based on the Modus Operandi (MO) of terrorist activities prevalent during the '80s and '90s and failed to adapt to the present-day tactics of extremist organisations. This disconnect underscores the necessity for security measures to be flexible and adaptive to the dynamic threat landscape.

*“A static programmatic approach is largely being used to manage a dynamic threat, which will inevitably leave gaps, which can expose the enterprise to unplanned disruption. Furthermore, such an approach can run the risk of wasting scarce security resources, with limited evaluation of whether historical controls are still valid.”*

**Simon Mann, Former Head of Risk for RNLI**

Given the dynamic nature of the security landscape, it's imperative for security professionals to adopt a proactive approach to effectively manage both present and emerging security risks.

Security personnel in corporate environments must leverage a data-driven, risk-led approach to anticipate and manage potential disruptive events. This strategy not only minimizes costly downtime but also equips business leaders with the necessary information for real-time decision-making. Such informed decision-making can empower leaders to drive business growth, safeguard the organization, and ensure a legal Duty of Care to their employees.

*“Driving your security function using a risk-based approach is the key to truly engaging as a business partner rather than being considered an overhead function strictly.*

*But fully embracing risk management means you also need a reasonable way to measure and report on the risk environment.*

*Digitalization is the next iteration of ESRM and security reporting generally. It is the piece of the puzzle that allows the security function to take all of the data generated by the tactical security activities and turn them into a usable picture to communicate the impact of security on the mission of the organization.”*

**Rachelle Loyear, Co-author. Enterprise Security Risk Management: Concepts and Applications**

# Why is Standardising Your SRM Process Beneficial?

Standardising your security risk management (SRM) process goes beyond simply securing your organisation. It involves making sense of the security context within your organisation and ensuring it aligns with it’s overall goals.

The advantages of a risk-based security approach allow security practitioners to connect with the business using language that resonates with the decision-makers. This approach pushes the security function to step away from being just a checklist-driven operation and instead actively engage with the organisation and its stakeholders.

Executing an effective risk assessment lies at the heart of this engagement, which can be achieved by answering three basic questions:

A picture containing text, circle, font, screenshot

Description automatically generated

Figure - SRA made simple.

Interacting in this way fosters a comprehensive understanding of the organisation's mission, values, operations, and goals. As security leaders understand where and how they can add value, the whole organisation will begin to acknowledge the pivotal part the security department plays.

*“Security threat & risk assessment and an understanding of ‘risk management’ should be key competencies for all security managers and leaders. However, a lack of a consistent standard approach means that these core skills are often overlooked, and they are not practiced enough throughout security functions.”*

**Paul Winstanley, Director Risk Management - Security Program Manager, WTW**

Additionally, transforming the security function from a cost centre to a data-informed, risk-oriented business ally empowers decision-makers to take advantage of opportunities that might have previously seemed too complex without specialist security risk insight. This transformation underlines the real value of the security function.

A picture containing windmill, wind turbine

Description automatically generatedThe contemporary risk management approach recognises both risks and opportunities. For example, in the energy sector, security professionals need to adjust their conventional focus on hydrocarbon energy security to consider the risks and rewards related to renewable energy sources like wind, solar, and wave power.

By standardising risk identification and devising effective risk mitigation strategies, security professionals can pivot quickly, enabling businesses to capitalise on new opportunities in this sustainable energy era.

**In doing so, the SRM process becomes an essential tool for**

**driving innovation and growth.**

# What Does Digitalisation Mean?

Digitalisation, as defined by the Gartner glossary, is the adoption of digital technologies to transform a business model, creating new revenue streams and opportunities. Essentially, it's about transitioning to a digital business model.

In a 2018 article, Forbes magazine highlighted a report by McKinsey & Company, noting that businesses investing in digital transformation and altering their strategies have seen productivity growth through increased revenue and returns on digital investment.

**Without a similar digitisation of SRM (Security Risk Management), businesses risk falling behind, unable to take full advantage of these valuable opportunities.**

By questioning conventional practices and understanding the business's operations, comprehensive security programs, encompassing both physical and digital realms, can provide enhanced insights. This improves overall safety and adds value beyond the traditional isolated, checklist-style risk management practices.

Businesses today are constantly striving for optimal efficiency and precision, adopting data-driven digital processes to attain this level of performance. However, in this age rich with data, the volume of information available can be daunting.

The corporate security function must evaluate threats, analyse risks, and formulate effective mitigation strategies in real-time. In doing so, these functions can become more flexible, incorporating pertinent data into their comprehensive SRM approach.

*“Digital transformation is key [to] place data, automation and tech at the heart of our operation to create an integrated risk management approach, maximize barrier strength and efficiency. Our vision: A digitally transformed, remarkably effective and agile team providing strategically aligned risk management outcomes for EY UK&I.”*

**Mark Spandler, Business Resilience Leader, Risk Management Ernst and Young LLP**

**Why has the adoption of digital approaches been slower within enterprise security functions?**

In 2018, Microsoft and Accenture conducted a "Future of Physical Security" survey involving two hundred senior physical security leaders across various industries. The results showed varied levels of digital maturity, with some sectors lagging by a decade. The respondents pinpointed "reactive threat management" and "intuition-led decision-making based on subjectivity" as the most significant challenges facing physical security operations today. Such challenges can make proactive action difficult, potentially putting people, brand, and reputation at risk.

In a conversation with a senior security leader from the energy sector, who had explored the hesitancy of corporate security professionals to embrace data-driven analysis for his MBA thesis, an interesting observation came up. He discovered that numerous security professionals who transitioned to corporate security as a subsequent career after honing their fundamental skills in the military, law enforcement, or government sector were unfamiliar with utilising readily accessible technology. Consequently, they often need help comprehending the advantages of a digital approach.

However, the tide seems to be turning as more early adopters of data-driven security risk management come through degree-level security risk management programs and professional development training courses advocating for standardisation and the use of technology.

**We are now witnessing the entry of a new, tech-savvy generation of security professionals into the sector.**

# What are the Advantages of Digitalising Your SRM Process?

## Significant Time Efficiency

Among security leaders' most prominent challenges are resource limitations and budget constraints.

**Security leaders are constantly being challenged to do more with less.**

A security leader from a prominent professional services company indicated that he simply doesn't have sufficient manpower to maintain a practical overview of the company's safety and security risk profile and manage these risks effectively.

To illustrate the impact of digitalisation on efficiency, we compared the time required to manually carry out an ISO-standardised security risk assessment using spreadsheets versus a digital SRM platform.

**The results were remarkable. Our analysis showed that a digital approach could reduce the time taken to create an initial assessment by up to 64%, and astonishingly, it could save up to 89% of the time required to update it.**

For a business managing the security of ten sites, the results demonstrate that adopting a digital SRM approach could provide the equivalent of two additional months of productivity per year, for less than the cost of two weeks' salary.

*“Substantiated threat data improves business risk intelligence enabling global consistency. The digitalization of the SRA process identifies business and operational risk metrics at both macro and micro levels, creating a permissive environment for projects to be successful, providing a competitive advantage for the business as a whole.”*

**Declan Meighan, Jacobs Director, Security – EMEA & FSU Global Security & Resilience**

## Standardisation

**If you ask ten different security professionals to undertake a security risk assessment, you are likely to receive ten different outcomes.**

Many security professionals today move into corporate or organisational security as a second career, typically from uninformed or government roles. Consequently, each professional brings their own unique risk assessment methodologies that align with their previous occupations.

A former police officer might evaluate risk from a law enforcement angle, while a former military professional may approach risk from a 'commander's estimate' perspective.

However, neither of these views considers risks in relation to business objectives. The security function must embrace a uniform risk management approach that aligns with the overall enterprise risk management strategy of the business.

Effective risk reporting should be succinct and visual to allow business leaders to digest the information, facilitating prompt decision-making quickly. The era of extensive narratives has passed. In today's fast-paced environment, no one has the time to go through fifty pages of security risk analysis. Implementing a uniform risk approach ensures that all security team members consistently conduct SRAs. Consistency and accuracy in security risk reporting across the business portfolio will enhance trust and understanding with business leaders outside the security function.

## Compliance

Business organisations must adhere to various internal and external rules, standards, and guidelines. These compliance requirements help to standardise vital management procedures, like information security, health & safety, travel security, and the overall risk management approach used to manage risks throughout the enterprise.

A digital approach to Security Risk Management (SRM) facilitates the integration of compliance-driven requirements into the organisation's Enterprise Risk Management strategy.

**Risk-led compliance ensures that the security mitigation strategy is consistently adjusted to suit the ongoing risk environment in which the business operates.**

## Communication

Implementing a standardised security risk management strategy that aligns with business goals promotes a deeper understanding of the security function within the business and nurtures a better comprehension of the business within the security department.

This significantly enhances communication throughout the organisation. Devoting time to converse with business colleagues to gain detailed insight into an organisation's culture, operations, and key stakeholders is crucial before exploring protective strategies. This approach not only strengthens trust but also improves communication channels.

During an assignment with a UK-based Not for Profit operating in Africa, our role was to create a security risk management strategy that would allow them to expand their operational reach while managing risks within their particular risk tolerance.

By clearly understanding their mission, the risks they were exposed to, and their risk tolerance, we formulated a plan that improved decision-making and guided budget allocation. Regional country directors remarked on the efficacy of the security plan due to our thorough understanding of their role, culture, and objectives.

Cultivating and maintaining a consistent understanding and standardised risk reporting throughout the organisation is vital for security leaders to advise top management effectively.

A data-driven digital dashboard, available around the clock, supports the visualisation of pertinent data and enhances the communication and understanding of security risks across the organisation. This fosters cross-functional integration and boosts overall organisational efficiency.

## 

## Holistic security management

Cybersecurity has taken a front seat in corporate security in the current digital landscape. Yet, cyber and physical security often intersect, even though these two functions have traditionally operated in isolation. This has led to vulnerabilities in enterprises that can be taken advantage of.

Convergence has become an oft-used term in contemporary security risk management, defined as "the amalgamation of logical security, information security, physical and personnel security, business continuity, disaster recovery, and safety risk management."

Adopting a standardised approach to Security Risk Management (SRM) agreed upon by all security professionals could trigger integration via the collective identification of business risks, followed by a coordinated approach towards developing effective mitigation strategies.

**A holistic approach to security risk identification and collective management will close some of the gaps exploited by those intending to disrupt your business operations.**

*“Cybersecurity sits at the heart of security in the 21st century. The boundaries between physical, personal, information, and ICT security are becoming blurred as our cars, homes, and offices become connected. Understanding and managing security risks in this dynamic and integrated environment can only be achieved through digitalization. A new specialization in security risk management is being created under our very noses and our societies will need security professionals with deep expertise in big data science.”*

**Julian Talbot, Co-author of the book Security Risk Management Body of Knowledge**

## Continuity

At a Security Risk Management (SRM) workshop hosted by Shell in 2015, the security team expressed significant concerns about training. They outlined the issue of 'skill fade' in relation to annual security risk reporting, indicating the need for readily accessible training to supplement initial training in SRM procedures and regular refresher courses to support annual security risk assessment updates.

A few years later, similar challenges were echoed during a discussion with a US-based International Non-Governmental Organisation (INGO). Despite having a highly global workforce, they had yet to instil a universal standard for security risk management throughout the organisation.

Implementing a common digital learning environment can address these standardisation and consistency issues. This allows security analysts to be trained consistently and access refresher training as needed, ensuring the quality and accuracy of regular risk reporting.

## Digital SRM Integration with ERM

A picture containing circle, screenshot, graphics, cartoon

Description automatically generatedImplementing a Digital SRM approach ensures comprehensive security consideration across all aspects of your business. But the gold standard would be to integrate this into the business's broader Enterprise Risk Management (ERM) strategy.

Many businesses have invested, or plan to invest, in a digital ERM or Governance, Risk & Compliance (GRC) platform and hope to utilise it for Security Risk Management.

Nonetheless, employing an ERM/GRC platform doesn't effectively facilitate the identification and management of security risks for security practitioners. Those who attempt to use it this way may experience a significantly diluted output of security risk, leading to considerable gaps in the organisation's security infrastructure.

The solution lies in integrating specialist safety and security risk management platforms with an ERM platform via a Common Data Environment (CDE). This allows risk managers to view a unified risk input without compromising the identification and analysis of security risk.

Investing in Digital SRM will enhance an organisation's digital ERM approaches, thereby boosting overall risk management efficiency, promoting cross-functional cooperation, and realising cost savings that lead to a short-term Return on Investment.

**Digitalisation paves the way for a more efficient approach to risk management, which not only bolsters business protection but also enables opportunities that the business may have otherwise avoided.**

*“The disparate nature of security risk reporting means that all too often cyber security risk and physical security risk managers use different platforms and the risks cannot be easily prioritized. In a single digital environment all security risks can be included, analyzed, and allocated to the right stakeholders and team (s). Digitalization can enhance the efficiencies of reporting as volumes of data are more effectively managed across organizational silos. The value of the digitalization of SRM is that it brings these previously disjointed processes into one environment for all to assess.”*

**James Willison, Founder, Unified Security Ltd.**

# Answering the Challenges of Modern Security Professionals

|  |  |
| --- | --- |
| A picture containing font, symbol, logo, graphics  Description automatically generated | **Consensus.**  Adhering to a risk-based strategy, in line with business risk standards, can aid in translating the traditional security lingo into business-friendly language. This strategy accentuates the need to understand the context of security within the business it is intended to safeguard. |
| A group of people with bubbles above them  Description automatically generated with low confidence | **Staffing.**  Like other business functions, security leadership constantly faces the challenge of maximizing output with fewer resources. Investing in an appropriate digital risk management solution could potentially save up to 80% of the time needed for manual implementation, at a fraction of the cost of additional personnel. |
| A calculator and a stack of coins  Description automatically generated | **Financial Constraints.**  Adopting a risk-led approach to security guarantees strategic allocation of resources to protect those elements most closely aligned with vital business objectives. This safeguards them against both existing and emerging threats, optimizing budget and resource usage and aligning them with real-time business needs and risks. |
| A picture containing symbol, sketch, font, logo  Description automatically generated | **Standardisation.**  An effective security risk management strategy must align with the business's enterprise risk management approach. Digitizing this agreed approach can drive efficiency and aid in maintaining continuity and improving communication. |
| A picture containing circle, symmetry, line, design  Description automatically generated | **Compliance**  Compliance standards, such as information security or site security standards, can be integrated into your digital Security Risk Management (SRM) platform. This integration fosters a risk-led compliance strategy, allowing control evaluations in line with the dynamic risk profile of the business. |
| A group of white speech bubbles  Description automatically generated with low confidence | **Communication.**  Security professionals must interact directly with the business to grasp its mission, culture, and key objectives. They must be capable of discussing security risk in context, in a language that business leaders understand, focusing on risk, business impact analysis, and cost-benefit analysis. |
| A black and white illustration of a court building  Description automatically generated with low confidence | **Governance**  Aligning security risk management with the business's mission, key objectives, and processes, especially enterprise risk management, enables security to integrate with the broader governance structure of the business. This approach positions security as a value proposition rather than a cost center. |

# Summary

The dynamic risk evaluation method I applied in Ethiopia took minutes, but it was convincing enough to prompt my client, of just two weeks, to effectively withdraw from their core role in the election observation mission.

**Standardising security risk management (SRM) amplified my communication skills with my clients.**

The digitisation of the SRM approach equips security professionals to manage current and emerging global threats targeting the organisation's critical assets across multiple jurisdictions. This approach leverages the vast amount of digital data available to produce precise analyses that business leaders require to make pragmatic, real-time decisions.

In our ever-evolving world, persisting with a programmatic, analogue approach to security management prevents security professionals from accessing the wealth of available data and the technical efficiency required to analyse it.

Data-driven, standardised, digital SRM bolsters the security of the business, along with the people and critical assets that support it.

The efficient and effective SRM output empowers senior management to grasp opportunities that may be missed by your competitors, thereby demonstrating the value the security function adds to the business.

**Traditional security methods will leave gaps that can be exploited, reinforcing the notion that your next threat is analogue.**

Data-driven digitalisation security risk management will:

* Enable real-time decision-making.
* Unlock opportunities.
* Strengthen convergence/integration/unification of the organisation's security functions
* Promote the integration of SRM with ERM, elevating security to top-table decision-making.

**Effective risk-led, holistic security management will drive growth and make your organisation safer!**

# About the Author

A person smiling in front of a snowy mountain

Description automatically generated with low confidencePaul Mercer is a seasoned international security and risk management specialist with a track record that spans across continents. He's the Founder and Managing Director of HawkSight Security Risk Management Ltd, a firm recognised for its award-winning innovative digital security risk management software.

Having worked in high-profile roles in regions like Asia, the Middle East, and Africa, Paul has managed crisis situations, executed high-risk evacuations, and advised global corporates and major events on security matters. He has also served in the Royal Navy as a helicopter observer.

Paul studied international politics outside his corporate roles, earning a master’s degree from the University of Glasgow. His leadership, strategic insights and innovative thinking have earned him recognition as a Certified Security Professional in the security industry, particularly for his work on digital risk management software solutions.

In addition to his professional pursuits, Paul is an avid sports enthusiast. He enjoys trail running, triathlons, skiing, and scuba diving. He lives in the French Alps with his wife Lizzy, daughter Chloé and Bernese Mountain dog Koda.

Logo

Description automatically generated

Text

Description automatically generated

*Nothing in life is risk-free, but risks can be managed. It’s our job to make everyone and everything safer.*

*HawkSight software uses a sophisticated algorithm that assesses risks based on relevant threat data. This delivers a dynamic risk profile, identifies vulnerabilities, and provides options for mitigation.*

*We call it security risk insight, and we’re global leaders at it.*

*We believe this will enable people to live freer lives and enterprises to flourish as risk diminishes.*

*The ability to live and operate safely in an increasingly complex world is our goal.*