AN INVESTIGATION INTO APPLICATIONS FOR CyBOK WITHIN THE INTERNATIONAL BUSINESS ANALYSIS COMMUNITY

MARK CROSS, ENVISTA CONSULTING LTD.

MARCH 2025

CONTENTS

1 EXECUTIVE SUMMARY

1.1 BACKGROUND AND CONTEXT

In an increasingly digital business environment, organizations rely on business change professionals, including business analysts, project managers, and practitioners of agile methodologies, to drive technological and operational improvements. These professionals play a critical role in shaping digital transformation initiatives, but they often lack formal training in cybersecurity principles, which can allow security risks to be introduced through change processes.

The **Cyber Security Body of Knowledge (CyBOK)** was developed to provide a comprehensive framework of cybersecurity knowledge, primarily for specialists in the field. However, its applicability to professionals specialising in fields outside of cybersecurity, particularly those working in business analysis and change management, remains underexplored. Many cybersecurity decisions occur outside of dedicated security teams, yet existing cybersecurity frameworks often assume that those engaging with them already possess a strong technical background. As a result, professionals who do not specialize in security may struggle to access and apply relevant cybersecurity knowledge effectively.

Recognizing this gap, this study explores whether and how CyBOK can be leveraged to enhance cybersecurity awareness among change professionals. By assessing current knowledge gaps, examining real-world challenges faced by these professionals, and evaluating CyBOK's accessibility, this research seeks to identify opportunities for improving its usability in a business-facing context.

1.2 OBJECTIVES OF THE STUDY

This research aims to:

- Identify and characterise the types of change professionals relevant to this research, including their roles, responsibilities and cybersecurity knowledge needs.
- Understand the interactions of these change professionals with security teams and their influence on cybersecurity decision-making within organisations.
- Assess how CyBOK aligns with these needs and identify accessibility barriers that prevent change professionals from effectively using it.
- Propose adaptations and/or extensions to CyBOK that would enhance its accessibility for non-specialists.

By addressing these objectives, this study seeks to bridge the gap between cybersecurity knowledge and business change practices, ultimately improving the security posture of organizations undergoing digital transformation.

1.3 KEY FINDINGS FROM INTERVIEWS

Interviews with 20 professionals across diverse industries, including finance, telecommunications, retail, academia, and cybersecurity consultancy, revealed consistent themes regarding the relationship between cybersecurity and business change.

The following insights were particularly notable:

1. **The Identity and Role of Cybersecurity Business Analysts**
   Cybersecurity-focused business analysis is a relatively new discipline, with professionals often transitioning into these roles through trial and error rather than by following a systematic process. Organizations increasingly seek BAs with security knowledge, but structured pathways remain lacking.
2. **The Role of Change Professionals in Cybersecurity Risk Management**
   Many BAs and PMs struggle with risk management because cybersecurity risk frameworks are not designed for business teams. They need structured approaches to assess risks in ways that align with business priorities.
3. **Complexity and Accessibility of CyBOK for Business Professionals**
   While CyBOK was not intended for an audience of business professionals, and it appears that it is seen as being too complex to use by non-security professionals, there are opportunities for resources which make CyBOK accessible for this wider audience. Respondents suggested role-specific guides, interactive content, and structured learning pathways to make it more accessible and relevant to change professionals.
4. **The Disconnect Between Business and Security Teams**
   Security and business teams often work in silos, leading to friction. This is consistent with arguments within the Security Economics Knowledge Guide 1.0.0 (Moore, 2024). Security professionals prioritize risk, while business leaders focus on efficiency, creating misalignment unless security is framed as a business enabler.
5. **The Need for Soft Skills in Cybersecurity Collaboration**
   Effective cybersecurity collaboration depends on strong stakeholder engagement and communication. Change professionals help bridge the gap between security and business, ensuring security concerns are framed in a business-friendly way.
6. **Cybersecurity as a Late-Stage Consideration:**
   Several respondents noted that security was frequently treated as a reactive rather than proactive element in projects, leading to delays, increased costs, and avoidable security gaps. The lack of early engagement between change professionals and security teams exacerbated these risks.

These findings reinforce the need for additional materials, developed to be supplementary to CyBOK, giving change professionals accessible, practical, and relevant guidance, informed by the knowledge and best practice defined by CyBOK.

2 INTRODUCTION

2.1 SCOPE OF THIS RESEARCH: THE GAP BETWEEN CHANGE PROFESSIONALS AND CYBERSECURITY

Cybersecurity is no longer confined to dedicated security teams; it is a fundamental component of business resilience, digital transformation, and regulatory compliance. As organizations expand their digital footprints, cyber threats increasingly target business processes, supply chains, and human factors rather than just IT infrastructure.

Change professionals, including business analysts (BAs), project managers (PMs), and other roles associated with change strategy and delivery, act as key facilitators of innovation and technological change but often lack structured cybersecurity training. Several industry frameworks acknowledge the importance of integrating security into business operations:

- The National Institute of Standards and Technology Cybersecurity Framework (NIST, 2024) emphasizes the need for cross-functional collaboration in managing cyber risks but does not provide explicit guidance for change professionals.
- ISO 27001 (ISO, 2022), the international standard for information security management, includes governance requirements but assumes implementation by security teams rather than business stakeholders.
- The NICE Cybersecurity Workforce Framework (NICCS, 2024) provides role-based cybersecurity skills mapping but does not explicitly define change professionals as a cybersecurity stakeholder group.

Due to these factors, cybersecurity remains an afterthought in many business transformation initiatives, with late-stage security interventions leading to costly delays. As one interviewee noted:

> *"Security is often seen as a blocker rather than an enabler. Business teams want to move fast, while security teams want to reduce risk. The challenge is finding a balance."*

This highlights the need for business-facing professionals to possess functional cybersecurity knowledge. These team members should not be expected to specialize in security, but they should be aware of how their decisions directly impact their organization's cyber risk posture. This study focuses on how these business-facing change professionals, and particularly Business Analysts (BAs), who bridge the gap between business needs and technology, are strategically placed to meet this need.

Key Responsibilities:

- Investigating Business Systems – Assessing structures, processes, and IT systems to identify areas for improvement.
- Defining Requirements – Documenting business needs to ensure IT solutions align with objectives.
- Facilitating Communication – Acting as a liaison between business stakeholders and technical teams.

Deliverables & Security Impact:

BAs produce Business Requirements Documents (BRDs), Process Models, and Risk Assessments, which influence security by:

- Ensuring security requirements are embedded in IT solutions.
- Identifying potential risks in business processes.
- Supporting proactive security measures through stakeholder analysis and workflow evaluations.

By integrating security considerations into their work, Business Analysts help organizations mitigate risks, protect data, and ensure resilient business operations.

2.2 THE CYBER SECURITY BODY OF KNOWLEDGE (CYBOK)

The Cyber Security Body of Knowledge (CyBOK, 2021) is a structured reference framework that provides a comprehensive overview of cybersecurity topics. The CyBOK and the associated Knowledge Guides and Topic Guides have been developed in collaboration with UK and international academic and industry partners to serve as a foundational knowledge base for cybersecurity education and workforce development. CyBOK is used to support academic programs, professional certifications, and practitioner training, offering a structured approach to cybersecurity concepts.

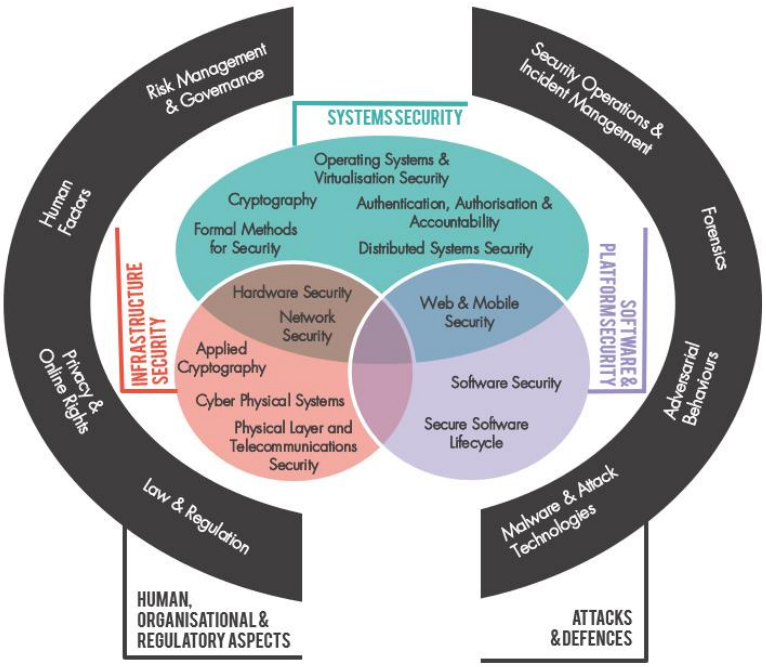

Figure 1 - The 21 Knowledge Areas (KAs) in the CyBOK Scope

It consists of an introduction and 21 knowledge areas, which are categorized into:

- Human, Organizational & Regulatory Aspects (e.g., risk management, governance, privacy laws).
- Attacks & Defences (e.g., malware, digital forensics, incident management).
- Systems Security (e.g., authentication, cryptography, secure operating systems).
- Software & Platform Security (e.g., secure coding, vulnerability management).

- Infrastructure Security (e.g., network security, cloud security, IoT security).

While CyBOK provides an authoritative foundation for cybersecurity knowledge, it was designed primarily for security professionals rather than non-technical business stakeholders. As a result, change professionals often find it difficult to navigate or apply in their work. However, the knowledge and practical guidance within CyBOK could be precisely what is needed to bridge this gap for change professionals, particularly as any material derived from CyBOK would support this group in developing well-informed and nuanced understanding of cybersecurity.

Several interviewees echoed this need:

> *"CyBOK is an excellent technical resource, but as a business analyst, I wouldn't know where to start. If there was a way to map it to my work, I'd be much more likely to use it."*

This study evaluates how the knowledge that is relevant to change professionals within CyBOK can be made more accessible to non-security professionals who require cybersecurity knowledge within a business context.

2.3 PROBLEM STATEMENT

Despite the growing emphasis on cybersecurity in regulatory compliance, risk management, and business resilience, change professionals often lack structured guidance on integrating security considerations into their work. This results in several key challenges, as reflected in participant interviews:

- **Limited Awareness of CyBOK:**
  Many change professionals interviewed were either unaware of CyBOK or found its content too complex for their needs. While cybersecurity experts viewed it as a valuable resource, non-specialist professionals struggled to identify the sections most relevant to their roles.
- **Barriers to Engagement with Cybersecurity Knowledge:**
  Interviewees described challenges in engaging with cybersecurity due to the technical nature of existing resources. Security teams often focus on in-depth technical implementations, whereas change professionals require security knowledge that aligns with business objectives, project lifecycles, and governance frameworks.
- **Cybersecurity as a Late-Stage Consideration:**
  Several respondents noted that security was frequently treated as a reactive rather than proactive element in projects, leading to delays, increased costs, and avoidable security gaps. The lack of early engagement between change professionals and security teams exacerbated these risks.
- **Need for Practical Guidance:**
  Interviewees expressed a desire for clearer, scenario-based guidance on how to integrate cybersecurity considerations into their work. They highlighted a need for structured pathways within CyBOK that map security knowledge to practical business applications.

These challenges indicate that while CyBOK is a rich knowledge source, its current format may not adequately serve professionals who require security awareness but are not dedicated cybersecurity practitioners.

3 RESEARCH METHODOLOGY

3.1 STUDY DESIGN

This study was designed as a qualitative research project to explore how CyBOK can be adapted to better serve business-facing change professionals. It employed semi-structured interviews with professionals across multiple industries, focusing on their cybersecurity awareness, engagement with CyBOK, and the challenges they face in integrating security into business change initiatives.

The research followed a three-phase approach:

1. **Engagement Phase** – Identification of expert participants and preliminary discussions.
2. **Data Collection Phase** – Conducting structured interviews across different professional roles and industries.
3. **Analysis Phase** – Thematic coding and synthesis of findings to identify key patterns and insights.

3.2 RESEARCH QUESTIONS

This study seeks to answer the following primary research questions:

1. How do business-facing change professionals engage with cybersecurity knowledge?
2. What are the key barriers preventing them from using CyBOK effectively?
3. Which cybersecurity concepts are most relevant to their roles?
4. How can CyBOK be adapted to improve accessibility and applicability for non-security professionals?

3.3 PARTICIPANT SELECTION & PROFILES

3.3.1 Sampling Methodology

Participants were selected through purposive sampling, focusing on individuals with direct experience in business change, cybersecurity, or both. The study aimed to capture diverse perspectives across industries, geographies, and roles.

- **Inclusion Criteria:**
  - Professionals in business analysis, project management, or related change delivery roles.
  - Experience in managing or influencing cybersecurity-related decisions.
  - Industry representation across multiple sectors (finance, retail, technology, academia, and consulting).
- **Exclusion Criteria:**
  - Individuals without exposure to cybersecurity considerations in their work.
  - Purely technical cybersecurity specialists without business change experience.

A total of 20 professionals were interviewed, representing:

- Business Analysts (BAs) – Change professionals responsible for defining project requirements and governance.
- Cybersecurity Professionals – Subject matter experts assessing security risks in business processes.
- Project Managers (PMs) – Facilitators of change initiatives with oversight on security integration.
- Academics & Industry Standards Experts – Researchers and contributors to cybersecurity knowledge frameworks.

A breakdown of participant roles, industries, and locations is summarized in Table 1 below.

ROLE	INDUSTRY	REGION	NO. OF PARTICIPANTS
Business Analysts & Change Coordinators	Financial Services, Consulting, Public Sector	UK, USA, Australia, UAE	8
Cybersecurity Professionals	Retail, IT, Telecommunications	UK, Europe, Hong Kong, New Zealand	6
Project Managers & Transformation Leaders	Healthcare, Government, Energy	USA, UK, Australia	4
Academic & Standards Experts	Universities, Cybersecurity Bodies	USA, Australia, UK	2

Table 1- Participant Distribution

Further information about participant profiles can be found in Appendix A.)

3.4 DATA COLLECTION & ANALYSIS

3.4.1 Data Collection Method

- Semi-structured interviews were conducted over a period of four weeks.
- Interviews were held via video conferencing and email correspondence where necessary.
- Each interview lasted between 30 to 60 minutes, allowing for deep discussions.
- Responses were transcribed and anonymized to protect confidentiality.

Interview topics covered:

- Awareness and perceptions of CyBOK.
- Experiences in cybersecurity-related decision-making.
- Challenges in integrating cybersecurity within business change initiatives.
- Recommendations for improving CyBOK's usability for change professionals.

3.4.2 Data Analysis Method

The study employed thematic analysis for identifying patterns within qualitative data.

1. Familiarization with Data – Initial reading of transcripts to identify recurring themes.
2. Coding & Categorization – Assigning labels to data extracts related to cybersecurity knowledge gaps, CyBOK's accessibility, and business-security alignment.
3. Theme Identification – Grouping similar responses into key themes aligned with the research questions.
4. Review & Refinement – Iterative refinement of themes to ensure clarity and consistency.

3.4.3 Key Analytical Themes Identified

Four principal themes were identified and these findings informed the subsequent analysis on how CyBOK can be adapted to bridge knowledge gaps in business change roles.

THEME	DESCRIPTION
Awareness Gaps	Low familiarity with CyBOK among business professionals.
Perceived Complexity	CyBOK content seen as too technical for non-specialists.
Security as a Late-Stage Concern	Cybersecurity often addressed reactively, not proactively.
Need for Practical Guidance	Demand for real-world case studies and structured learning pathways.

Table 2 - Key Themes Identified Within Transcripts

3.5 ETHICAL CONSIDERATIONS

This study adhered to ethical research guidelines, ensuring:

- Informed Consent: Participants were briefed on the study's purpose and data usage.
- Confidentiality & Anonymization: No personally identifiable data was included in the analysis.
- Data Protection: All transcripts and notes were securely stored and accessible only to the author.

3.6 SUMMARY OF RESEARCH APPROACH

- Balanced sample of business change professionals and security experts to assess CyBOK's applicability.
- Qualitative Study using semi-structured interviews with 20 professionals across industries.
- Thematic Analysis to extract patterns related to cybersecurity engagement and CyBOK usage.
- Ethical Research Practices ensuring confidentiality and data security.

4 FINDINGS & ANALYSIS

This section presents the key findings derived from 20 semi-structured interviews conducted with professionals across business change, cybersecurity, and industry standards domains. The findings are categorized into four major themes that emerged through thematic analysis of participant responses.

4.1 LIMITED AWARENESS OF CYBOK

A significant number of business change professionals were unaware of CyBOK before this research. In contrast, cybersecurity professionals were more familiar with it and recognized its value as a technical reference. However, many acknowledged that CyBOK is not widely known outside the cybersecurity community.

> *"I've been working in business change for 15 years, and I deal with security concerns regularly. But I hadn't even heard of CyBOK until you mentioned it."*

Several participants suggested that CyBOK's visibility needs improvement within non-security disciplines such as business analysis, project management, and enterprise transformation.

> *"If there was a way to embed CyBOK into existing business change certifications, people like me would come across it sooner."*

However, a counterpoint was raised by some cybersecurity professionals, who argued that CyBOK's primary audience is intended to be security practitioners rather than generalists.

> *"CyBOK was never meant to be an introduction to cybersecurity—it's a deep knowledge resource for professionals who already understand security."*

This contrast in perspectives highlights an opportunity to reach a broader audience, via ancillary materials which will help to support an expanded community of CyBOK-informed change professionals.

4.2 BARRIERS TO ENGAGEMENT WITH CYBERSECURITY KNOWLEDGE

From the interviews conducted, several key challenges emerged that prevent change professionals from engaging with cybersecurity knowledge effectively:

For participants who were introduced to CyBOK during this study, the most common challenge was its technical complexity. Change professionals found it difficult to identify relevant content without a cybersecurity background.

> *"CyBOK is structured for security experts—it assumes you already know what you're looking for. I wouldn't even know which section to read as a business analyst."*

Additionally, some interviewees noted that security teams often communicate cybersecurity risks in overly technical terms, making it difficult for change professionals to engage meaningfully.

> *"Security teams tell us about 'threat actors' and 'attack vectors'—but what does that mean for a project timeline or a business requirement?"*

A counterpoint came from cybersecurity experts who believe that change professionals should take more initiative in developing cybersecurity literacy, rather than expecting security teams to simplify content for them.

> *"If you're making decisions that affect cybersecurity, you have a responsibility to upskill yourself. Security can't always be simplified for every audience."*

This divergence in viewpoints suggests a mutual gap in expectations—change professionals seek simplified, business-aligned security knowledge, while cybersecurity experts expect them to develop a baseline understanding before engaging. It was observed that existing cybersecurity training is split across two extremes:

- Highly technical content (e.g., ethical hacking, penetration testing, cloud security) that is not relevant to business-facing roles.
- High-level governance courses (e.g., ISO 27001 Lead Auditor, CISM) that focus on compliance rather than practical decision-making within change initiatives.

> *"Most security certifications are aimed at CISOs or engineers. There's nothing structured for business analysts or project managers."*

The IIBA Certified Cybersecurity Analyst (CCA) credential attempts to bridge this gap, but interviewees noted that it has not been updated in several years.

4.3 NEED FOR PRACTICAL GUIDANCE

Several interviewees emphasized that security guidance should be structured around real-world use cases rather than theoretical concepts.

> *"Give us case studies, examples, scenarios. If we see how security failures have impacted other organizations, we'll learn much faster."*

A recurring theme across multiple interviews was the need for practical, scenario-based cybersecurity guidance that aligns with business decision-making.

> *"Security training often feels abstract. If we had real-world business examples of security failures, people would take cybersecurity more seriously."*

Several participants suggested that CyBOK should include structured pathways tailored to different roles within business change.

> *"Give me a 'Business Analyst's Guide to Cybersecurity'—something that tells me exactly what I need to know."*

However, some cybersecurity professionals cautioned against oversimplifying cybersecurity concepts, emphasizing that depth is necessary to ensure accurate risk management.

> *"If you simplify security too much, you lose critical details. Risk assessments need to be rigorous, not just high-level business advice."*

This tension suggests that CyBOK should offer both simplified guidance for business professionals and deep technical knowledge for specialists, rather than a one-size-fits-all approach.

To make CyBOK more actionable for change professionals, it may be beneficial to:

- Develop tailored learning pathways for business analysts, project managers, and transformation leaders.
- Develop resources which illustrate how to apply CyBOK principles to risk-based decision-making.
- Provide real-world case studies demonstrating the consequences of poor cybersecurity integration in business change initiatives.

4.4 CYBERSECURITY AS A LATE-STAGE CONSIDERATION

Several participants reported that cybersecurity is still perceived as a function handled by dedicated security teams, rather than an organization-wide responsibility. This often leads to a reactive approach, where security is considered only after major project decisions have been made.

> *"BAs, PMs, and architects should engage with security early, but in reality, they don't. It's often left to the security team, who then come in too late to change the course of a project."*

This siloed approach results in:

- Security being treated as a compliance hurdle rather than an integral part of transformation.
- Late-stage security interventions leading to delays, cost overruns, and increased risk exposure.
- Inadequate communication between security and business teams, leads to poor project decision-making.

One of the most frequent concerns expressed by interviewees was that cybersecurity is often introduced too late in the business change process, leading to delays, cost overruns, and security gaps.

> *"By the time security gets involved, the budget is spent, the deadlines are fixed, and there's no flexibility. At that stage, security feels like an inconvenience, not a priority."*

Several participants from business change roles noted that they were rarely given security-related training, leading to missed security risks in early-stage planning.

> *"If no one has told me what security concerns to look for, I won't raise them in a requirements document. It's as simple as that."*

However, a cybersecurity expert provided a different perspective, suggesting that many organizations lack the right governance structures to engage security teams early.

> *"It's not just about awareness—it's also about governance. If security isn't mandated as part of the approval process, it will always be treated as an afterthought."*

This highlights the need for both process improvements and better training to ensure that cybersecurity is embedded earlier in business change projects.

5 RECOMMENDATIONS & OPPORTUNITIES FOR INCREASING CYBOK'S IMPACT

The findings from this study suggest that CyBOK has significant potential to support business-facing change professionals in developing cybersecurity awareness if accessibility and applicability could be improved for non-specialists. This section outlines potential avenues that CyBOK's stakeholders may wish to explore further to enhance its impact for a broader audience. These recommendations offer CyBOK stakeholders the opportunity to lead the cybersecurity conversation within other professional domains.

5.1 ENSURING A BALANCE BETWEEN ACCESSIBILITY AND TECHNICAL DEPTH

Some cybersecurity professionals in the study expressed concern that oversimplifying security concepts for non-specialists could lead to misinterpretation or inadequate risk management.

> *"It's a fine balance—make security too simple, and people misunderstand the risks. Make it too complex, and they won't engage at all."*

If CyBOK is expanded to support a broader audience, a balance may need to be struck between accessibility and technical precision. Potential approaches for consideration might include:

- Layered Content Approaches – Offering introductory explanations for business professionals, with deeper technical content for those needing further detail.
- Contextual Framing of Security Concepts – Explaining cybersecurity risks in terms of business impact, rather than purely technical threats.
- Maintaining CyBOK's Technical Integrity – Ensuring that content remains rigorous while still being adaptable for different audiences.

This balance may help retain CyBOK's credibility as a cybersecurity reference while making it more approachable for business change professionals.

5.2 INVESTIGATING ROLE-SPECIFIC LEARNING PATHWAYS WITHIN CYBOK

Some interviewees suggested that structured learning pathways within CyBOK could help non-specialists quickly identify content relevant to their roles.

> *"If CyBOK had a 'Business Analyst's Guide to Security Risks' or a structured way to identify what's relevant to my role, I'd be much more likely to use it."*

One option that CyBOK's maintainers may wish to explore is whether role-specific content guides could be developed to highlight security topics most relevant to business change professionals. Possible areas of focus might include:

- Risk Management for Change Professionals – Guidance on mapping cybersecurity risks to business impacts.
- Cybersecurity in Project Governance – Security considerations for Agile, Waterfall, and hybrid project methodologies.
- Security Implications of Digital Transformation – Frameworks for embedding security into cloud, AI, and automation initiatives.

If pursued, this approach might help non-technical professionals find relevant cybersecurity knowledge more efficiently, improving engagement with CyBOK as a reference tool.

5.3 EXPLORING THE USE OF PRACTICAL, SCENARIO-BASED LEARNING RESOURCES

Many interviewees emphasized that real-world case studies are among the most effective ways for non-specialists to develop cybersecurity awareness.

> *"Case studies. That's what we need. If we could see real-world examples of security failures in business change projects, we'd learn much faster."*

One possible avenue for exploration is whether additional practical resources—such as case studies, worked examples, or interactive learning tools—could be developed to complement existing CyBOK content. Potential areas of focus might include:

- Examples of security failures in business change initiatives – Illustrating the consequences of overlooking cybersecurity in projects.
- Best practices for bridging the gap between security and business teams – Demonstrating effective collaboration in real-world scenarios.
- Interactive tools for assessing security risk in business contexts – Helping professionals identify and mitigate risks relevant to their industry.

If feasible, such resources could help change professionals apply cybersecurity principles in a way that aligns with their day-to-day responsibilities.

5.4 EXPLORING THE EXPANSION OF CYBOK'S CERTIFICATION MAPPING TO INCLUDE BUSINESS CHANGE CERTIFICATIONS

CyBOK has already undertaken a mapping initiative that aligns its content with a range of professional training programs and academic certifications in cybersecurity, as detailed in the CyBOK Mapping Booklet v2.2 (CyBOK, 2024). This effort has helped learners and employers identify how cybersecurity knowledge aligns with structured education pathways. This exploration may also help build stronger links between cybersecurity and business change

disciplines, ensuring that CyBOK's resources are discoverable by professionals who make security-impacting decisions but do not work in technical cybersecurity roles.

5.5 ENCOURAGING EARLIER CYBERSECURITY INTEGRATION IN BUSINESS CHANGE

A common challenge highlighted by participants was that cybersecurity is often considered late in the change lifecycle, leading to delays and costly rework. Some organizations have attempted to address this by introducing structured security review points within project workflows.

> *"Security should be part of the conversation at the beginning of a project. But instead, it's treated as a compliance check at the end, which causes major delays."*

Organizations looking to improve early-stage cybersecurity integration may wish to explore:

- Security Awareness Checklists for Business Change Professionals – Simple prompts to help project teams consider security risks during early planning.
- Risk-Driven Decision Frameworks – Approaches that help business analysts and project managers factor cybersecurity into risk assessments.
- Collaborative Security Reviews – Mechanisms for bringing security and business teams together before project decisions are finalized.

While CyBOK itself does not dictate implementation methodologies, stakeholders may consider whether existing CyBOK content could be linked to industry-recognized security governance models, helping organizations integrate security more effectively into business change processes.

6 CONCLUSION

This study has explored how the knowledge contained in the Cyber Security Body of Knowledge (CyBOK) could be made accessible for business-facing change professionals, including business analysts, project managers, and transformation leaders. Through 20 semi-structured interviews across multiple industries, the research identified four key challenges that may impact engagement with CyBOK:

1. Limited Awareness of CyBOK – Many change professionals had not encountered CyBOK before this study, while cybersecurity experts recognized its value as a technical reference.
2. Barriers to Engagement with Cybersecurity Knowledge – The technical depth of CyBOK made it difficult for non-specialists to identify relevant information without prior cybersecurity expertise.
3. Need for Practical Guidance – Participants emphasized that real-world case studies, role-specific guidance, and scenario-based learning would make CyBOK more applicable to their work.
4. Cybersecurity as a Late-Stage Consideration – Many business change professionals noted that security is often introduced late in projects, leading to delays and security gaps.

The research findings suggest that there may be opportunities to expand CyBOK's reach by exploring ways to create useful additional materials to enhance its accessibility for non-technical professionals. These opportunities include:

- Creating an adjunct mapping booklet, analogous to the CyBOK Mapping Booklet, to identify connections between professional certifications in business analysis, project management and IT governance , and CyBOK.
- Developing role-specific learning pathways guidance to help change professionals identify relevant cybersecurity knowledge more efficiently.
- Exploring the use of real-world case studies and interactive resources to help non-specialists understand security risks through practical examples.
- Creating supplementary materials, balancing accessibility with technical depth, to ensure that the knowledge derived from CyBOK remains rigorous while being approachable for broader audiences.

While this study provides insights into how change professionals engage with cybersecurity knowledge, it also highlights the need for ongoing discussions and collaboration between cybersecurity and business disciplines.

Ultimately, ensuring that business change professionals have access to structured, role-relevant cybersecurity knowledge could lead to more secure digital transformation initiatives, reduced security risks, and stronger alignment between security and business teams. The CyBOK community may wish to explore the feasibility of these recommendations further, considering how best to balance CyBOK's role as a technical reference with providing materials for the evolving needs of professionals who influence cybersecurity decisions in non-specialist roles.

This research provides a foundation for further exploration, and future studies could assess the impact of any potential adaptations, ensuring that CyBOK and the associated materials continue to serve as a valuable resource for a broad range of cybersecurity stakeholders.

7 BIBLIOGRAPHY

CyBOK. (2021). *The Cyber Security Body of Knowledge v1.1.0.* Retrieved from https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK. (2024). *Mappings of University and Professional Training Programmes to CyBOK, Version 2.2.* Retrieved from https://www.cybok.org/media/downloads/CyBOK_MappingBookletv2.2_2024.pdf

ISO. (2022). *ISO/IEC 27001:2022.* Retrieved from https://www.iso.org/standard/27001

Moore, T. (2024). *Security Economics Knowledge Guide Issue 1.0.0.* Retrieved from https://www.cybok.org/media/downloads/Security_Economics_KG_v1.0.0.pdf

NICCS. (2024). *NICE Workforce Framework for Cybersecurity*. Retrieved from https://niccs.cisa.gov/workforce-development/nice-framework

NIST. (2024). *National Institute of Standards and Technology, Cybersecurity Framework* . Retrieved from https://www.nist.gov/cyberframework

SFIA. (2024). *SFIA-9 Home*. Retrieved from https://sfia-online.org/en/sfia-9

APPENDIX 1 – PROFILES OF INTERVIEW SUBJECTS

Subject ID	Pseudonymised Job Title	Pseudonymised Organisation	Location	Interview Date
#01	Consultant	Cybersecurity Consultancy	UK	11/02/2024
#02	Global Lead	IT Educational Standards Body	UK	31/01/2025
#03	Enterprise Security Architect	British University	UK	04/02/2025
#04	Business Analyst	Local Council	UK	06/02/2025
#05	Regional Director for EMEA	Professional Association for Business Analysts	UK	13/02/2025
#06	Head of Cybersecurity	Cybersecurity Consultancy	UK	25/02/2025
#07	Head of Security Business Engagement	Major UK Retail Chain	UK	27/02/2025
#08	Senior Information Security Risk Officer	Multi-National Banking Group	Lithuania	19/02/2025
#09	Data Management Consultant	Financial Services Company	USA	14/02/2025
#10	Standards Development Manager	Cybersecurity Professional Association	USA	21/02/2025
#11	Senior Director, Standards and Practice	Cybersecurity Professional Association	USA	21/02/2025
#12	Standards Manager	Cybersecurity Professional Association	USA	21/02/2025
#13	Senior Director, Digital & ERP Cybersecurity	Medical Technologies	USA	25/02/2025
#14	Associate Professor	US University	USA	03/03/2025
#15	Associate Professor in Cyber Security and Privacy	Australian University	Australia	20/01/2025
#16	Head of IT	Logistics Company	Hong Kong	19/02/2025
#17	Senior Technical Business Analyst	Telecommunications Company	New Zealand	30/01/2025
#18	Business Analysis Consulting Manager	Major Multi-National Consulting Company	New Zealand	05/02/2025
#19	Vice President, Business Enablement and Transformation	Major Multi-National Banking Group	UAE	26/02/2025
#20	Business Analyst	Bank of New Zealand	Australia	30/01/2025