Defend Against Global Cybercrime by Unlocking the Power of Business Relationship Management

Empower the CISO with BRM

Authors:

John Lieberwerth, BRMP ICT2Business

Peter Lijnse, MBRM Lead the pack consulting

Date: March 5, 2024

A shocking statistic found in a study by the A. James Clark School Center for Risk and Reliability at the University of Maryland showed that hackers attack every 39 seconds, and according to IBM's Cost of a Data Breach Report 2023, the global average cost of a data breach was $4.45 million. This is why in most organizations, it no longer applies that 'information supports the business' but rather 'information *is* the business.' In today's digitally driven landscape, information security has risen to become a fundamental pillar of organizational stability and resilience. However, in Splunk's 2023 CISO report, only 47% of the CISO's polled answer directly to their CEO. Additionally, while 86% of CISO's say they feel their biggest responsibility is to ensure their board sees security as a valuable investment, they struggle to get them to see past basic regulatory compliance to organization-wide security best practices and success metrics.

Information security is the responsibility of the entire organization, which means it needs to be clearly communicated and the correct actions are taken. It is important that all stakeholders are aware of the risks and measures that need to be taken to ensure the confidentiality, integrity, and availability of information. Management has an important role in this by developing policy and setting guidelines. In addition, it is important that sufficient resources are available to take the necessary measures. It is also important to regularly evaluate whether the measures taken are still sufficient and to make adjustments where necessary. In short, information security is a joint responsibility of the entire organization, this is where a Business Relationship Management capability is required to be successful.

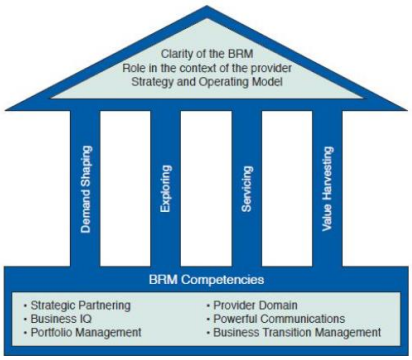
Yet, a persistent challenge looms large, threatening the very integrity of information security – **the glaring lack of robust relationships and effective collaboration between various departments and groups within an organization**. Even the U.S. Government has acknowledged this shortcoming, with the U.S. Government Accountability Office sharing recently that one department admitted that it took five months to be briefed after a breach was identified. This disconnect fuels a growing sense of urgency and frustration among cybersecurity professionals. They are acutely aware of the potentially catastrophic consequences of isolated, siloed efforts when confronted with relentless cyber threats.

The Chief Information Security Officer (CISO) is responsible for the organization's information security policy. The CISO defines the information security policy, sets up the information security organization, determines the resources required, and their deployment on concrete security

measures. The CISO ensures an appropriate level of information security and information security behaviour in the organization based on the needs and risk appetite of the organization. The CISO is regarded by internal and external stakeholders as the expert in the field of information security. The CISO reports hierarchically and functionally to the organization's Board of Directors and carries out the tasks independently.

The CISO needs different types of support for those tasks to perform well. This includes support from management, technical support from the IT department, financial resources, and the cooperation of all employees. Properly developing and making maximum use of these four forms of support can be a major task. This is a bottleneck that many CISOs struggle with.

For example, look at the role of employees who need guidance and direction from their CISO: they must adhere to the organization's information security policy and the procedures and guidelines contained therein. They should also be alert to potential security risks and report them to the appropriate person or department. Employees must also be regularly trained and informed about information security to keep their knowledge and skills up to date. In short, employees are an important link in the information security chain and must be aware of their roles and responsibilities. A CISO who has to do all this alone has a major challenge.



The house of BRM

Amidst this backdrop of urgency and frustration, a crucial leadership cap
ability emerges: business relationship management (BRM), which is *a role, function, and organizational capability*. BRM serves as the vital link between information security teams and other organizational units, facilitating the essential connections and collaborative spirit required to navigate the intricate cybersecurity landscape successfully.

In the rapidly changing landscape of information security and cybersecurity, insufficient time is invested in analyzing developments. Responding to changes requires quick decision-making, clear communication, and smooth cooperation. BRM continuously proves its worth in these important aspects. BRM promotes collaboration, helps break down silos, and stimulates communication and collaboration.

CISO Challenges and Their Impact on the Organization

The CISO stands at the center of this increasingly complex, rapidly changing digital landscape and is confronted with new technologies, cyber threats, compliance, and regulations. This makes the role of the CISO increasingly challenging. The CISO must now not only ensure basic security but also think more strategically and proactively respond to changing risks, tasks, and responsibilities.

This creates pain points that directly affect the organization in terms of knowledge acquisition, behavioural changes, and general organizational conditions. These challenges include (these challenges are further defined in the table in the next section):

- **Lack of Support from Middle Management –** The absence of backing from middle management can hinder knowledge dissemination and behaviour change.
- **Limited Mandate –** A limited mandate restricts the CISO's ability to influence organizational behaviour.
- **Slow Decision-Making from Management –** Delayed decision-making can result in inadequate responses to security threats.
- **Limited Resources –** Insufficient resources may impede knowledge acquisition and behaviour change efforts.
- **Perceived Lack of Strategic Importance –** When the CISO role is not seen as strategic, it can undermine efforts to drive behaviour changes and improve security practices throughout the organization.
- **Communication with Stakeholders –** Neglecting communication with stakeholders can limit the organization's understanding of security initiatives.

In addressing these challenges, organizations can proactively promote knowledge gain, foster behaviour changes, and enhance overall conditions to build a robust security posture.

Connection Between Business Relationship Management and Information Security Management

According to the Business Relationship Management Institute, **business relationship management capability** is everything it takes, both visible and invisible, to nurture relationships in an organization. This refers to the skills, knowledge, and behaviours necessary to effectively manage and nurture relationships between different business units. It involves the ability to understand the needs, goals, and expectations of various partners and to converge those with the strategic objectives of the organization.

A BRM capability helps promote a culture within the organization that's based on collaboration, trust, creativity, innovation, authenticity, and shared ownership. When this capability is well-developed, it brings different teams together to create comprehensive strategies that benefit the organization and produce meaningful results.

The BRM capability can help to solve the challenges for the CISO of getting the organization to better understand the need and priority of required measures. Especially business relationship managers can support clear communication with other parts of the organization.

What the Strategic BRM Capability Provides to the CISO

Establishing a strategic BRM capability can be instrumental in supporting the CISO in effectively communicating with executive management and defining the mandate, budget, and decision-making speed. In the following table, the CISO challenges are defined and show how a BRM capability can help alleviate these challenges.

CISO challenges and BRM capabilities

Challenge	Description	BRM Capability
Lack of Support from Middle Management	The absence of backing from middle management can hinder knowledge dissemination and behaviour change, as it may lead to a disconnect between strategic security initiatives and day-to-day operational practices.	**Advocacy and Influence:** BRM can work closely with middle management to advocate for the importance of security initiatives and their alignment with broader organizational goals. By building strong relationship networks and focusing on collaboration, BRM can help bridge the gap between security strategy and day-to-day operations, encouraging middle management to support security efforts.
Limited Mandate	A limited mandate restricts the CISO's ability to influence organizational behaviour, potentially impeding efforts to instill a security-conscious culture.	**Aligning Objectives:** BRM can collaborate with the CISO to identify opportunities to align security objectives with other business objectives. By demonstrating how security supports the organization's broader goals and has an impact on the overall conditions of the organization, BRM can help expand the CISO's mandate and influence.
Slow Decision-Making from Management	Delayed decision-making can result in inadequate responses to security threats, impacting the organization's ability to adapt swiftly and make informed decisions.	**Data-Driven Insights:** BRM can provide decision-makers with data and insights on the potential risks and consequences of delayed decisions related to security. This can help accelerate decision-making by highlighting the urgency of security concerns.
Limited Resources	Insufficient resources may impede knowledge acquisition and behaviour change efforts, making it challenging to implement comprehensive security measures.	**Resource Allocation:** BRM can assist the CISO in making a strong business case for adequate resources by demonstrating the return on investment in security. BRM can also explore opportunities for cross-functional resource sharing and collaboration. The CISO and BRM can jointly consider whether a budget for information security and cybersecurity can be determined and allocated for organizational units and

Challenge	Description	BRM Capability
		whether that is better than placing one general budget for IS with the CISO. When budgeting per organizational unit, the CISO is primarily the strategic advisor for management. The organizational units will then be given responsibility for their own IS budget. This can be a strong incentive to think carefully about what to invest in and to make a result obligation clearer and enforce it.
Perceived Lack of Strategic Importance	When the CISO role is not seen as strategic, it can undermine efforts to drive behaviour changes and improve security practices throughout the organization.	**Strategic Alignment:** BRM can work with the CISO to emphasize the strategic importance of cybersecurity in achieving the organization's goals. This includes regularly communicating the impact of security on the organization's reputation, customer trust, and competitive advantage.
Communication with Stakeholders	Neglecting communication with stakeholders can limit the organization's understanding of security initiatives and impede the necessary behavioural shifts.	**Stakeholder Engagement:** BRM can help the CISO improve communication with stakeholders by identifying key stakeholders and their needs, developing tailored communication strategies, and ensuring that security initiatives are effectively communicated throughout the organization.

In essence, a strategic BRM capability can facilitate collaboration between the CISO and other parts of the organization. It helps in translating security priorities into business value and impact, building relationships, and ensuring that security is integrated into the organizational culture and decision-making processes. This collaborative approach can enhance the CISO's ability to address the mentioned challenges and create a more security-conscious and resilient organization.

How a BRM Capability Can Work Together With CISO

As seen in the previous table, the strategic BRM team collaborates closely with the CISO team and other C-level executives to ensure the convergence of security goals and broader business objectives, striving for seamless alignment of security initiatives. Additionally, their role involves identifying key stakeholders across various business units and departments, cultivating strong relationships with them to grasp security needs. Furthermore, the BRM team assumes responsibility for establishing strategic communication channels and educating business stakeholders on the significance of cybersecurity, emphasizing their pivotal role in sustaining a secure environment. Equally important is their involvement in shaping ideas, integrating security considerations into

business initiatives from inception by collaborating with project teams. Lastly, maintaining a feedback loop between the CISO team and business units remains essential, with the BRM team actively collecting input on security processes and policies, using this feedback to enhance security strategies and effect necessary adjustments.

A strategic BRM team plays a pivotal role in bridging the gap between information security and broader business functions. Their primary aim is to ensure that security efforts closely align with business priorities while fostering a culture of collaboration and shared responsibility for cybersecurity.

BRM role: handles organizational groups

It is important to note that BRM has traditionally focused on introducing the BRM role or a BRM team in an organization. This role or team handles relationships between two or more organizational groups. Often, the business relationship manager represents one group and cultivates relationships with other groups. However, not every organization requires a dedicated BRM team. It is possible to introduce a strategic BRM capability as part of existing leadership teams with a focus on building collaborative partnerships with business units. This can offer valuable support to a CISO team.

There are different ways BRM can be utilized by CISO. Consider the following to get the value out of a BRM capability for a CISO and their Information Security group.

- **Utilizing an Existing BRM Team:**
  One approach for IS to collaborate with BRM is by leveraging an existing BRM team within the organization. This option offers several advantages, including resource efficiency, as it doesn't require the creation of a new department. Existing BRM professionals typically have experience in fostering relationships with various departments, which can be invaluable in aligning information security with broader business objectives. Additionally, integrating into an established BRM capability may be a faster approach compared to setting up a new team. However, there are challenges to consider. Existing BRM teams often have a multitude of responsibilities, potentially resulting in competing priorities. This can make it challenging to allocate sufficient attention and resources to information security. Moreover, BRM professionals may lack the specialized knowledge required to fully grasp the nuances of information- and cyber security, which requires additional education and coaching.
- **Establishing a Dedicated BRM Team for Information Security:**
  Another option is for the CISO to establish a dedicated BRM team specifically tailored to the needs of information security. This approach allows for a more precise alignment of BRM capability with security goals. The team can be staffed with individuals who possess a deep understanding of information security, reducing the knowledge gap and ensuring that security-related initiatives are prioritized.

Nevertheless, there are challenges associated with this option. One significant challenge is the cost involved in creating and maintaining a dedicated team, which can be particularly burdensome for smaller organizations with limited budgets. Resource availability can also be an issue, as finding or allocating resources for this purpose may be difficult. Integrating the new team smoothly into existing organizational structures can be complex, requiring careful planning and coordination. This option can also create confusion with business units when there are multiple BRM teams.

- **Enhancing Relationship Management within Information Security:**
  An alternative approach involves strengthening relationship management skills within the existing IS team. This option focuses on developing the abilities of security professionals to build and maintain collaborative partnerships with other departments. It can be a flexible and cost-efficient approach, particularly suitable for organizations with limited resources. However, this approach comes with its own set of challenges. Developing relationship management skills and processes within the existing team can be time-consuming, and the benefits may not be realized immediately. Staff may also initially resist changes in their roles and responsibilities, which can slow down the process. Additionally, while information security professionals can become proficient at relationship management, they may still lack the specialized expertise and time in BRM that dedicated teams possess.

The choice among these options should be made based on the organization's size, budget, existing resources, and the level of integration required to effectively align information security with the broader business objectives and strategies. Each option has its unique advantages and challenges, and the decision should align with the organization's specific needs and circumstances.

Conclusion

Business Relationship Management (BRM) plays a crucial role in enhancing information security within organizations. Information security is a key component of organizational stability, the lack of collaboration and effective communication between departments poses a significant threat. This disconnect not only undermines security efforts but also fuels frustration among cybersecurity professionals.

The Chief Information Security Officer (CISO) plays a pivotal role in implementing security measures but often faces challenges due to a lack of defined role and support, limited mandate, slow decision-making, and insufficient resources. These challenges hinder the organization's ability to respond effectively to security threats and to cultivate a security-conscious culture.
BRM emerges as a vital leadership capability in this context. It serves as the connector between information security teams and other organizational units, fostering the relationships and collaboration needed to navigate the complex cybersecurity landscape. BRM promotes a culture based on trust, creativity, innovation, authenticity, and shared ownership, which is essential for effective information security management.

The strategic BRM team works closely with the CISO team, aligning security goals with business objectives and establishing communication channels with key stakeholders. They play a key role in integrating security considerations into business initiatives and maintaining a feedback loop to enhance security strategies.

For CISOs, utilizing BRM can take various forms, including leveraging an existing BRM team, establishing a dedicated BRM team for information security, or enhancing relationship management skills within the information security team. Each approach has its advantages and challenges, and the choice depends on the organization's specific needs, size, budget, and existing resources.

In closing, BRM is invaluable for ensuring information security excellence. It not only facilitates better communication and collaboration across departments but also ensures that information security strategies are integrated and aligned with the broader business objectives. By harnessing the power of BRM, organizations can significantly enhance their information security posture, making them more resilient against the ever-evolving cyber threats.

CALL OUT BOX: Tips for CISO

As a CISO, your role extends far beyond technical security implementations. To effectively address today's complex security challenges and lead your organization towards a robust security posture, consider actively collaborating with a Strategic Business Relationship Management (BRM) capability. Here's why:

1. **Broader Business Impact:** A strategic BRM capability can help you bridge the gap between security and the broader business objectives. They enable you to demonstrate how security initiatives align with organizational goals, making a compelling case for security investments.
2. **Influence and Mandate:** Partnering with BRM expands your influence within the organization. They can work with you to extend your mandate by showcasing the strategic importance of security, enabling you to drive behavioural changes and instill a security-conscious culture more effectively.
3. **Resource Optimization:** BRM can assist in optimizing resource allocation. By presenting data-backed insights on the ROI of security investments, they can help secure the necessary resources for comprehensive security measures.
4. **Communication Excellence:** Collaborating with BRM ensures effective communication with stakeholders. They assist in tailoring your messages, identifying key stakeholders, and ensuring that security initiatives are clearly understood throughout the organization.

Peter Lijnse. MBRM

Peter is an experienced Business Relationship Management (BRM) leadership coach, speaker, author and facilitator. He helps organizations to develop a BRM capability and coaches leaders on how to get the most out of their BRM capability. He co-wrote with Elka Schrijver a book on 'Leading with Impact'. Peter has worked in various industries and is a sought-after speaker on Business Relationship Management.

'Leaders must possess Business Relationship Management as a crucial leadership skill. Fostering BRM knowledge and behaviour among organizational leaders through collaborative relationship-building is essential for results that have value and impact for the organization.'

John Lieberwerth, BRMP *BSc in Business informatics*

Three decades of experience in IT, in various executive and managerial positions. Over the past three years, the emphasis has been on information security, cybersecurity and privacy.

The reason for writing this article is the experiences of CISOs in their daily practice in which they are confronted with obstacles that put pressure on the performance of their work and job satisfaction. For me, the bridge to relationship management was already laid eight years ago. At that time, I found all kinds of opportunities in BRM to allow the two worlds of IT and Business to work together. 'Convergence' is the key word. After studying CISM and based on practical experience, I believe that CISOs can benefit greatly from the possibilities that BRM as role, function and organizational capability.