Business Information Security Officer (BISO) Program and Role

Prepared by the FS-ISAC Business Security Executives Forum

FS-ISAC

BISO Program and Role

Executive Summary

This paper examines the Business Information Security Officer (BISO) program and role from the perspective of practitioners in the financial services sector, offering insight into the value proposition, organization, responsibilities, and challenges of the role. It is not an implementation guide.

BISOs are an important part of an organization's cybersecurity function. As a liaison between cybersecurity and the business, BISOs ensure that the enterprise's information and technology assets are secure, that its business requirements are received and understood by cybersecurity, and that the business understands local cybersecurity risks. BISOs' in-depth knowledge of and alignment to the business allows organizations a more proactive approach to cybersecurity and greater trust among key stakeholders, more effective use of security resources, and solutioning better tailored to the firm's environment and goals.

The BISO role requires technical expertise, communication skills, executive presence, and relationship management abilities. A BISO's responsibilities include ensuring cyberthreats are properly mitigated, consulting on security controls, collaborating on regulatory compliance and employee training, supporting third-party risk management, and more. They must stay abreast of their business, technologies, risks, policies, standards, and baselines, which requires constant learning.

Definitions

- **Business/lines of business/business units:** Corporate subdivisions focused on a single product or family of products serving a particular company need or customer transaction.
- **Cybersecurity**: Team responsible for protection and restoration of, and preventing damage to, computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
- **Enterprise**: A legal entity possessing the right to conduct business on its own.
- **Partners**: Individuals, entities, or business units with functional expertise in one or more areas related to the enterprise.
- **Risk** (cyber, technology, etc.): A measure of the extent to which an entity is threatened by a potential circumstance or event. It's typically a function of the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs and the likelihood of its occurrence.

The alignment and reporting structure for BISOs relates to the institution's size, industry, and culture, but typically BISOs' alignment is either functional (aligned with a line of business or department), product-oriented (such as cloud, M&A, computer networks, etc.), geographical, or the role may combine these elements. Ideally, a BISO should report directly to the CISO and be dotted-line to their business leader, viewed

as a “mini CISO” with the autonomy to act within the bounds of approved cybersecurity policy and standards.

Depending on the alignment and structure of the BISO role, its challenges can include shifting responsibilities and “scope creep,” lack of clarity around the purpose of the role and metrics of success, internal politics, and lack of authority.

There are no developed metrics specific to the BISO role, but success could be defined in terms of meeting business objectives in a secure and compliant way. To help the BISO, organizations should develop a clear BISO objective, commit to the BISO’s success and use data to track it, provide appropriate communication channels, offer learning opportunities, and provide a diverse and inclusive support team able to address all situations.

Audience

- Chief Information Security Officer (CISO)/Chief Information Officer (CIO)/Chief Risk Officer (CRO)/C-level executives considering implementation of a BISO program or challenged with their program’s relationship with the business.
- Business executives faced with a challenging, ever-evolving cyber threat and risk landscape that requires divisional specific oversight and a need for direct partnership with cybersecurity.
- BISO leaders considering refinement of their BISO program.
- Cybersecurity professionals interested in a BISO role.

BISO Program and Role

Overview

Business and technology organizations are moving faster than ever. Emerging technologies accelerate the pace of change. This speed drives a need to mature the security capabilities of business and technology teams and ensure a close partnership with cybersecurity. The BISO plays an important part in that. This document details the BISO function and how it can help enable the business to meet its objectives securely.

The BISO's business alignment and in-depth business knowledge enables cybersecurity to take a more proactive approach to engaging the business. These relationships allow cybersecurity to see across the horizon and engage on projects while they are still ideas, dramatically reducing the cost of security and increasing its effectiveness by integrating cybersecurity rather than adding it on at the end.

BISO responsibilities vary widely between business sectors but at a high level, core BISO attributes relate to:

- Business cybersecurity accountability – BISO's align and engage with the business to foster knowledge of the people, objectives, challenges, and planned work that may affect cyber-risk. The BISO shares responsibility with business unit leaders in ensuring compliance of cybersecurity policies, local regulations, and oversight of cybersecurity efforts that enhance both divisional and corporate security.
- Managing cyber-risk – BISOs serve a strategic leadership function responsible for consultation with business leaders in identifying cybersecurity risk and supporting management of those risks. BISOs don't own the risk – they help define, communicate, escalate, and govern when necessary. Ultimately, the business owns the risk.
- Consulting and advising – The BISO is responsible for delivering cybersecurity domain counsel to both business leaders and cybersecurity teams, from answering questions to deep-dive engagements on key business and technology initiatives.

Expectations of the BISO Role: Manage, Model, and Assess

> Engagement with risk management
> Incident management
> Threat modeling
> Vulnerability management
> Third-party assessments
> Security awareness programming

BISO Program and Role

BISOs can serve as a liaison between teams, providing partnership and direction and building trust, which is critical to the organization's ability to simultaneously move quickly and manage risk. Cybersecurity organizations are very complex and highly specialized with their own jargon, objectives, and way of thinking about the world. Business teams have their own terminology, motivations, and accountabilities. These differing outlooks hinder trust and can leave business and technology teams confused and frustrated. By translating "security and compliance speak" into meaningful guidance and real-world recommendations, BISOs help achieve business requirements while leveraging state-of-the-art cybersecurity solutions.

By providing full context, the BISO is a multi-directional conduit, uniting cybersecurity, business, and technology teams. And by translating and clarifying the words, actions, and motives of different teams, BISOs build trust between team members.

Expectations of the BISO Role: How BISOs Build Trust

The following concepts are adapted for the BISO role from "The Trust Equation," developed by Charles H. Green, David Maister, and Robert M. Galford.

- Credibility: The BISO builds trust by being a credible cyber expert and by talking credibly about the business, its objectives, and its challenges.
- Reliability: The BISO builds trust by making cybersecurity easier to understand and more consistent. When partners are unsure, they can talk to their BISO. When partners are confused or unsatisfied with the answer from cybersecurity partners, they can talk to their BISO. This consistent point of interaction, attuned to goals and objectives, creates reliability and latterly, trust.
- Psychological Safety: The BISO builds trust by demonstrating empathy for the challenges business partners face, along with a balanced approach to risk management that acknowledges cyber-risk is not the only business risk.
- Self-Orientation: The BISO builds trust by acknowledging that perfect security isn't the primary goal of the organization -- business value and other business risks are reasonable considerations in a balanced decision.

The Business Problems BISOs Solve

The role of a BISO is to provide specific, business-focused, proactive threat management. By liaising with the CISO's representatives and other technology teams, BISOs help the business understand local cybersecurity risks.

BISOs collect, process, and analyze data and information to develop recommendations and cybersecurity direction based on risk and business input, which directly relate to the business unit being supported – e.g., adjust control tolerances to meet business needs, while ensuring the controls remain properly balanced with cybersecurity's requirements. This tailored information drives improved decision-making in consideration of the specific threat landscape, people, processes, and systems related to the business.

The BISO role should be positioned to assist the design and implementation of cybersecurity policies, procedures, and guidelines within the correct context for each line of business.

Expectations of the BISO Role: Risk Profile Escalation

By implementing a BISO model, the risk profile of business teams can be escalated into the enterprise. Enterprises without BISOs tend to create programs, processes, and systems at the enterprise level, with little or no input from functions and business teams.

Take, for example, a large business line with multiple legacy systems needing to protect existing systems and implement new solutions. The BISO would analyze the business line's IT and business strategy, then advise on ways to optimize information security costs and investments in alignment with business strategy – not just control risks to secure end-of-life systems.

The objective is to ensure effectiveness of security resources while assisting the business in meeting its goals.

Qualifications for the BISO Role

The attributes needed for the BISO role can vary depending on the seniority of the role in the organization. However, in general, the BISO role requires technical expertise, communication skills, executive presence, and relationship management abilities.

The BISO is an advocate for the business and ensures cybersecurity understands business requirements and challenges. BISOs also serve as cybersecurity representatives, driving the enterprise's cyber agenda into the business through implementation and facilitation. They oversee the cybersecurity related to the business/function, including relationships with third parties. Indeed, third-party solutions do not always meet security standards. In such cases, BISOs may consult

with providers to improve their products' security to enable the business functionality without increasing risk.

BISOs ensure that cybersecurity objectives and measures – as defined by the institution's information technology (IT) strategy, cybersecurity policy, and cybersecurity guidelines – are transparent within the institution and that compliance with them is reviewed and monitored regularly on an event-driven basis.

Further, the BISO provides holistic cybersecurity risk metrics and reporting to the business leadership, support of cybersecurity initiatives and tools to be adopted by the business, and cybersecurity incident support as directed by the security operations center (SOC) or incident commander.

Relationship Building

The BISO is there to evaluate, advise, partner, and support. To do so, the BISO must build solid relationships and become a trusted partner. Achieving this is not easy, but as the BISO is seen to deliver solutions rather than problems, partners tend to view the BISO as a critical resource.

Expectations of the BISO Role: Time Allocation

To address the needs of the business and security, as well as build relationships with the key stakeholders, BISOs spend much of their time in meetings – important since communicating and liaising are primary components of their job.

Communications

Solid communication skills are fundamental to the role – the BISO represents cybersecurity, technology, and/or the business teams to each other. Moreover, the BISO is often responsible for helping clients and suppliers understand the institution's current cybersecurity program, and for educating regulators on business-specific control frameworks.

The BISO must also communicate upcoming technologies, risks, policies, standards, and baselines to business and functional leaders. This educational communication can take many forms: newsletters, training sessions, or individual meetings. BISOs often partner with the cybersecurity training and awareness team or program to deliver cyber education to their business unit.

BISO Skills Development

A BISO should focus on continuous learning and development in various areas:

- **Cybersecurity:** Stay updated on the latest cybersecurity threats, trends, and best practices to effectively protect the organization's information assets.
- **Regulations and compliance:** Keep up with evolving data protection regulations and compliance requirements relevant to the sector and geographic region(s).
- **Risk management:** Enhance risk assessment, mitigation strategies, and incident response planning skills.
- **Business acumen:** Understand the institution's business processes, goals, and strategies to better align security efforts with its objectives.
- **Communication:** Improve communication skills to effectively convey complex security concepts to both technical and non-technical stakeholders and explain business topics to cybersecurity and information security professionals.
- **Leadership:** Develop leadership skills to lead and manage security teams, foster a security-aware culture, and gain buy-in from senior management.
- **Vendor management:** Learn how best to assess and manage third-party vendors' security practices to ensure the security of shared data and systems.
- **Security awareness training:** Participate in the creation and delivery of effective security awareness training for employees to reduce human-centric security risks.
- **Incident response:** Participate in the development and testing of incident response plans and after-action reviews (AARs) of incidents to improve efficiency of security incident handling and minimize potential damage.
- **Technical knowledge:** Stay knowledgeable about emerging technologies in cybersecurity, including identity and access management, cloud security, network architecture, and encryption methods.
- **Collaboration:** Build relationships with external peers and with internal departments such as IT, legal, and compliance to support a holistic approach to security.
- **Ethical hacking:** Gain insights into the TTPs used by malicious actors through ethical hacking and penetration testing.
- **Metrics and reporting:** Learn how to measure the effectiveness of security initiatives and present meaningful metrics to stakeholders. This is always evolving.
- **Privacy:** Understand the basics of privacy principles and regulations for the geographic region(s) and sector, particularly if the organization deals with personal data. Partner with the Chief Privacy Officer (CPO) or leader to support both business and cybersecurity initiatives that may overlap with privacy.
- **Continuity planning:** Collaborate with business resiliency leadership to support the development of strategies (business continuity and disaster recovery) to ensure minimal disruption during security incidents

Career Progression

While some BISOs orient toward leadership in the technology/CISO organization, others pursue a business leadership role.

Regardless of career trajectory, BISOs must engage in constant learning and stay abreast of industry changes. BISOs should take classes, attend conferences, obtain certifications (CISSP, CCSP, Project Management, CRISC, CISM, Security+), and build solid relationships across the organization – all critical elements of taking charge of a career.

Market Data on Salary and Factors for Salary Range:

The salary for a BISO varies according to location, industry, expertise, experience, and responsibility level. Organizations like IANS[i] provide market data on BISO salary range; however, job postings may provide more precise salary information.

BISO Skillset

The attributes below are examples of the skills and experiences BISOs need to effectively perform their job duties. Depending on organizational structure, positional authority, and seniority, BISOs may find graduate degrees, such as a Master of Business Administration (MBA), to be desirable. More senior BISO positions will require many or all of the skills and experiences listed here.

- Bachelor's degree in computer engineering/science or equivalent industry certifications
- IT/risk/security leadership experience
- 3 – 5 years' experience in a technology field
- Significant experience in more than one cyber domain
- 10+ years' experience working in IT/risk/cyber organizations
- 10+ years' experience in IT risk technologies, technology strategy, and/or technology operations. Experience includes managing and delivering IT services; IT analytics; enterprise applications; data/information management and information delivery applications; IT standards and methodologies.
- Exceptional strategic planning and relationship skills. BISOs must be comfortable managing and maintaining working relationships with senior executives internally and externally.
- Exceptional relationships with senior leadership/executives, as BISO's are seen as an extension of the CISO.
- Thought leadership and collaboration skills in technology operations and critical infrastructure. BISOs work strategically to find opportunities for growth and cost innovation.
- Strong communication and leadership skills. BISOs must articulate vision across teams and businesses to leverage partners to lead change.
- Ability to build a high-performance culture and the capabilities of employees and teams while leading change.
- Competitive drive to create efficiencies and drive costs down while generating value for clients and shareholders.

Assessing the Success of a BISO Program/Role

The success of the BISO program and role can be evaluated with various frameworks and models, such as the Capability Maturity Model Integration (CMMI) or the Gartner BI Maturity Model. These frameworks can help organizations understand how well the BISO is achieving their mission and identify what they need to do to improve their maturity level and achieve better results. Review Section 6: Metrics for additional information on how to measure the effectiveness of a BISO program.

Maturity Models

CMMI defines five levels of maturity for any process or program:

- Initial
- Managed
- Defined
- Quantitatively managed
- Optimizing

The Gartner BI Maturity Model focuses on the maturity of business intelligence initiatives and defines six levels of maturity:

- Unaware
- Reactive
- Proactive
- Managed
- Optimized
- Pervasive

BISO Alignment Model

It is critical to right-size the BISO role to the organization and evaluate it as the organization or regulatory environment changes. The specific alignment and reporting structure of BISOs within an enterprise can vary depending on the institution's size, industry, and culture, but close alignment to the team that the BISO supports is foundational to the BISO's success and effectiveness. This alignment can be based on one or a combination of the following:

- Functional alignment (line of business or department, i.e., consumer banking, commercial banking, corporate, investments, insurance, payments, etc.)
  - In organizations with multiple business functions (e.g., finance, HR, IT), BISOs may be aligned with specific functions rather than business units. For example, there could be a finance BISO, an HR BISO, and an IT BISO, each responsible for providing cybersecurity subject matter expertise and risk evaluation within their respective functional areas.
- Geographic alignment
  - In global enterprises, BISOs may be aligned geographically and are responsible for ensuring cybersecurity compliance and best practices within specific regions or countries, considering local regulations and risks.
- Product alignment (cloud, M&A, computer network, etc.)

- Some BISOs are aligned to products such as mergers and acquisition assessments, computer networks, or technologies (i.e., cloud). These BISOs have an in-depth understanding of the product and liaise with business-aligned BISOs to drive the right solutions for the business.

- Hybrid models
  - Many organizations combine elements of the above structures to best fit their needs. In these hybrid arrangements, BISOs may have a functional alignment but still report to the CISO for overarching security strategy and coordination.

Ultimately, the alignment of BISOs in an enterprise should strike a balance between providing specialized security expertise and ensuring that security measures are closely aligned with the business's objectives and success.

Expectations of the BISO Role: The Goal of the Structure

The specific structure should be tailored to the organization's unique needs, risk profile, and culture to effectively manage cybersecurity risks and provide a “check and balance” to CIOs. This can be done by building hard approval requirements into policy language. The goal is not to slow the business down, but to ensure cybersecurity is built into technology and\or business objectives.

BISO Reporting Structure

Regardless of the reporting structure, successful BISOs establish strong partnerships with the business units or functions they support. They must work closely with business leaders to understand the business' objectives, identify security risks, and develop security strategies that align with the organization's overall business goals. The BISO should have sufficent access to their aligned business unit to be aware of and familiar with its strategic objectives and have open lines of communication to their aligned risk owners.

It is important to note that, depending on the industry, regulators may have a say in the reporting structure as well as the BISO's remit and responsibilities. Additionally, there may be several levels of BISO within the same organization. See below for some examples of reporting structures:

Expectations of the BISO Role: Reporting Structure

The BISO's reporting structure depends on several factors including:

- Role and responsibilities of the BISO
- Size of the organization
- Culture of the organization
- Regulators' opinion and/or requirements
- Business strategic objectives

- **Report to the CISO or CIO:** BISOs provide specialized security guidance and support for specific business units or functions and report directly to the CISO, who is responsible for the overall cybersecurity strategy and program. In some reporting structures, the BISO reports to a Regional Information Security Officer, who then reports to the Cyber Information Security Office. In organizations with only one region, BISOs may report to a Senior BISO, who then serves the CISO.

- **Report to the risk organization:** BISOs report to the risk organization, which can include enterprise risk or technology risk.

- **Report to business unit leaders:** BISOs report to the leaders of the business units they support, such as a Product Manager (i.e., cloud, M&A, computer network, etc.), Product Security Manager, or their respective technology division. This reporting structure is more common in larger enterprises with decentralized structures, where each business unit has its own security needs and priorities. Reporting directly to a business unit leader integrates the BISO into the business unit teams, allowing the BISO greater insight into business technology and cybersecurity risk decisions. This arrangement ensures that security considerations are tightly aligned with the business' goals and operations.

- **Matrix reporting:** BISOs report to both the CISO for security expertise and guidance and to the leaders of their respective business units for operational alignment. This dual reporting structure allows BISOs to balance the needs of the business with security requirements.

Titles Used for the BISO

The functional and corporate titles of the BISO role are influenced by areas of focus, reporting structure, business alignment, responsibilities, and the organization's title nomenclature.

Nonetheless, the BISO is fundamentally responsible for helping the business manage risks. This is not limited to cyber-risks. Depending on the organization, BISOs can be responsible for cyber-risks, technology risks (which include cyber-risks, operational risks, technology resiliency, business continuity, etc.), regulatory risks, information security risks (which include cyber-risks, data loss prevention, privacy, etc.), and/or physical security risks.

As such, other titles used for the BISO role include Business Information Security Manager, Business Information Security Lead, Technology Risk Business Leader, and IT Risk Lead.

Expectations of the BISO Role: BISOs Are Not Project Managers

While a project management skillset helps BISOs succeed in the role, BISOs are not project or program managers for cybersecurity or other teams. BISOs can conduct oversight over projects and programs, and provide portfolio oversight at a strategic level, but project management is not a dedicated function of the role. There may be times when there is a gap and the BISO must assume duties as a project manager, but this should be a momentary role.

The title Business Information Security Officer is, however, the most appropriate to the role (unless regulatory requirements prohibit the use of "officer" as it can pertain to specific responsibilities and accountabilities in some industries and functions). Branding a BISO as a Risk Officer, IT Risk Lead, Technology Risk Professional, Governance Risk and Compliance Officer, or other "risk" related title could dilute the authority of the BISO and its clear association with cyber and information security.

The Ideal Structure

The ideal structure for a BISO role depends on the firm's business, market, organizational structure, regulatory environment, and risk appetite. As the chief cybersecurity and cyber-risk advisor to the business, the BISO logically reports directly to the CISO, the Divisional CIO/CEO, or both, dotted-lined to their business leader. That

enables BISOs to be part of the leadership team of the business unit and cyber operations. Ideally, the BISO is viewed as a "mini CISO," with the autonomy to act within the bounds of the approved cybersecurity policy and standards.

Importantly, the BISO should be independent and not a technology owner. That enables the BISO to provide accurate risk-based advice to the business without conflict of interest. Depending on the breadth and scope of the business or division the BISO is aligned to, a staff or a federated security team may be required. That team could either report directly to the BISO or be matrixed to the BISO for operational execution (i.e., Information Security Analysts, business\divisional employees with separate managers).

Expectations of the BISO Role: The BISO's Team

The composition of the BISO's support team depends greatly on the BISO's responsibilities, accountabilities, and goals. A strong data analytics position on the team is typical, however, as the BISO program's success depends on accurate reports of cybersecurity risk and activities.

Roles and Responsibilities

While a BISO may report into a variety of teams within the organization, the areas of focus for a BISO are fundamentally the same. These usually include:

- Cybersecurity threats: BISOs are expected to stay informed of evolving cybersecurity threats and the threat landscape as it relates to the business sector. In addition to ensuring that these threats are properly mitigated by the cybersecurity teams, BISOs should identify and facilitate the resolution, where practicable, of areas of potential issues or areas that suffer control weaknesses.

- Information security: BISOs, by definition, are responsible for the breadth of information security domains. They are accountable for providing consultation and/or oversight on controls, exemptions to controls or standards, and reviewing loss information to prevent similar incidents in the future.

- Regulatory compliance: BISOs should collaborate with legal counsel to ensure that the organization's cybersecurity program complies with various industry-specific regulations and data protection laws, such as NY Department of Financial Services Part 500 (PCI-DSS, NYDFS), Office of the Comptroller of the Currency Gramm-Leach-Bliley Act Appendix B (OCC GLBA), General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and more. BISOs should stay abreast of changing regulations, ensure the implementation of necessary controls to maintain compliance, and partner with organizational compliance teams.

- Employee awareness and training: BISOs are responsible for driving a strong security culture within the organization. As such, they often partner with the training and awareness department to help educate employees about security best practices and raise awareness about potential threats. BISOs may also conduct regular training sessions to ensure that employees understand their roles and responsibilities in maintaining information security.

- Third-party risk management: Many organizations work with external vendors, partners, or suppliers who have access to the institution's sensitive data or systems. Along with the third-party risk management teams, BISOs support business and cybersecurity teams in the assessment and management of the risks associated with third-party relationships, helping to ensure that these partners maintain a high level of security to protect shared information.

- Emerging technologies: Understanding emerging technologies helps BISOs forecast security implications and enables them to support the development of strategies to mitigate associated risks.

- Trusted advisor: The BISO acts as a trusted advisor to both the business and cybersecurity leadership, often as a single point of contact for cybersecurity communication across lines of business.

- Influence cybersecurity strategies and priorities: BISOs are in a unique position to determine how cybersecurity is aligned to a business' critical processes. When cybersecurity process and/or technology changes are created without BISO involvement, there is a greater likelihood that the changes may conflict with business processes and experiences, adding delays to adoption or negatively impacting the business and customers.

- Communicating to the business: BISOs may be relied upon to communicate and translate cyber intelligence and impacts to business leaders using the relationships they have built. While BISOs cannot be involved in every security decision, change, or proposed initiative, BISOs should partner with cybersecurity leaders to convey information in a timely manner for business response and adoption, and in language the business can understand.

Key Challenges and Obstacles

The way the BISO is positioned in the organization can be a determining factor in the challenges those in the role face. However, the following issues are common to BISO programs.

Shifting Responsibilities

The BISO role contains an element of variety, which can cause "scope creep." To avoid that, the scope and purpose of the BISO role/function should be well documented. Though BISOs typically engage on topics across cybersecurity domains and leverage subject matter experts as necessary, the BISO is not typically responsible for implementation of recommended security guidance and controls. The role should not be treated as a catch-all for miscellaneous cybersecurity administrative tasks.

Lack of Understanding About the BISO's Purpose

Unless the purpose and outcomes of the BISO role are communicated well and enterprise wide, employees may fail to understand the role's function and pull BISOs into processes so late the BISO can only course correct, escalate, or expedite.

For example, consider a business team implementing an AI project under the assumption that AI is a data quality solution outside the purview of cybersecurity. In fact, AI can impose significant risks. A BISO's input could enable the team to implement the AI solution within the business' risk tolerance, prevent remediation issues, and ensure the business impact of the technology.

BISOs should continuously engage with cybersecurity and business leadership via regular participation at cybersecurity and business unit staff meetings, business-line compliance and risk routines, one-on-ones with key relationship partners, presentations, industry engagement, and mentoring. BISOs should be aware of evolving organizational needs and adapt accordingly.

Navigating Internal Politics

The cross-functional nature of the role magnifies its susceptibility to internal politics. BISOs should prioritize understanding their organization's corporate culture and creating positive relationships, especially with the CISO, cybersecurity teams and leaders, and their business executives and stakeholders. The relationships with these partners can help BISOs navigate internal politics and set expectations for everyone involved.

BISOs should facilitate cybersecurity's communication to the business, explaining cybersecurity needs and giving ample lead time. Providing a strategic timeline for the business helps set expectations, encourages valuable feedback, and will help demonstrate security as an enabler instead of a blocker.

Lack of Authority

Structure and reporting lines can designed to give BISOs responsibility without authority. BISOs need the ability to advise and direct teams. Some BISOs are asked to drive results in their lines of business, and if they are not given authority or lack relationships with stakeholders, it is hard to get things done.

Improper Placement in the Organization

Some BISOs are layered under a Vice President (VP), which can direct them toward their VP's focus areas, rather than the full scope of the cybersecurity organization.

How to Measure Success

There are no industry-wide performance metrics defined specifically for the BISO role and they originate few projects or initiatives, making it hard to determine whether the completed work is the effort of the BISO or the project team.

However, given the role of the BISO as the chief cybersecurity advisor to the business, the BISO is critical in enabling the success of the business by helping to manage operational and cybersecurity risks. As a result, the BISO's (and cybersecurity's) strategic objectives should be aligned to the business' strategic objectives. The BISO's success could therefore be defined in terms of meeting business objectives in a secure and compliant way.

Methods of evaluating and measuring a BISO's performance can include the following examples:

- The number of audits supported/engaged on, if the BISO is responsible for supporting technology audits. Similarly, "Low Cyber Findings" could be a performance goal, if it conforms to the business leader's goals and is within the BISO's scope of responsibility.
- No past due security issues, indicating that identified security risks are well managed.
- Remediation status of penetration tests findings by line of business.
- Degree of involvement in supporting the line of business (e.g. relationship building), such as level of engagement in the appropriate meetings, working with the stakeholders, consulting on risk exceptions or acceptances, advising on regulatory alignment or proposed technology solutions, etc.

- Contributions to/outcomes from agreed upon objectives, projects (cybersecurity or business driven), and other initiatives where the BISO added value via their participation and engagement.
- Participation in training and development for themselves and extended to others (speaking, presenting, panelists, papers, and mentoring).
- Demonstrated decision-making maturity and ability to take on new and varied projects.
- BISO support for the Objectives and Key Results (OKRs) and Key Risk Indicators (KRIs) for cybersecurity teams and the lines of business related to cybersecurity, where appropriate.
- Success of the BISO's direct reports.

Supporting Resources

Certain resources provide foundational support that helps BISOs succeed.

A clear objective: Define the responsibilities of the BISO, keeping in mind alignment to the needs of the business and security. What problem(s) or challenge(s) is the BISO program meant to address? What is the BISO intended to accomplish?

Commitment to the teams' success: Address the BISO function's challenges, efforts, and values beyond greenlighting personnel or funding. A senior-level champion (i.e., CISO/cybersecurity and business leadership) is key, and support from the CIO and/or the executive leadership team is paramount.

Effective communication channels: Choose appropriate channels, methods, and styles for the target audience within your organization. Choosing the right channel and receiving feedback are fundamental to starting and running a BISO program.

Strategies to Gain Executive Commitment to a BISO Program:

Requests for commitment to a BISO program/role should align with, augment, and elevate the business and cybersecurity mission, vision, and objectives. Where feasible, use a data-driven justification to supplement the request, highlighting how the BISO or more BISO resources will result in a return on investment (return = speed or time gained, costs reduced or avoided, compliance improved, etc.). Highlight the cost of inaction, as well as the real-world "wins" of competitors.

Diversity and inclusion: BISOs will not have experience with every situation. Recognition and appreciation of the differences and similarities among team

members highlights the value of a variety of backgrounds, perspectives, experiences, and talents within the cybersecurity profession. Having a diverse and inclusive environment, promoting teamwork, and information sharing will help address challenges that inevitably arise.

Ongoing Learning

Acquiring new knowledge, skills, and attitudes helps BISOs grow and improve. Learning also supports innovation and the ability to continuously strive for better results. BISOs need access to team retrospectives and strategy planning, technical briefs from providers, participation in communities like FS-ISAC, briefings from experts, the ability to access educational resources, professional leadership development, etc.

BISOs also benefit from formal learning opportuniites. Many training options are available for BISOs to enhance their skills and knowledge, such as:

- Certifications: Industry-recognized certifications can provide comprehensive training. Some relevant certifications include Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA), and Certified Information Privacy Professional (CIPP).
- Workshops and seminars: Many organizations and training providers offer workshops and seminars on topics supported by BISOs, like risk management, security awareness, legal and compliance, incident response, cyber intelligence, or leadership skills.
- Online courses: Platforms like YouTube, Coursera, Udemy, and LinkedIn Learning offer a wide range of online courses on cybersecurity, risk management, leadership, and other relevant topics.
- Conferences: Attending cybersecurity and information security conferences can provide valuable peer networking opportunities and exposure to the latest industry trends or emerging topics.
- Vendor-specific training: Some vendors offer training or demonstrations of their security tools or platforms.
- Industry associations: Organizations like CISA, FS-ISAC, ISACA, ISC, and ISSA offer resources, training, and networking opportunities for cybersecurity professionals.

- **Local security groups:** Local cybersecurity meetups and groups (ex. ISACA, ISSA) enable BISOs to learn from peers and experts in their region/city, often across industries/sectors.
- **Books and publications:** Books, articles, and publications related to information security, cybersecurity, risk management, business sector, and leadership can provide valuable insights into trends and tactics, techniques, and procedures (TTPs).
- **Cybersecurity challenges and competitions:** Participating in capture the flag challenges and other cybersecurity competitions hones practical skills. Participation can also surface opportunities to mentor others or simply provide insight into cybersecurity incident response team (CIRT) challenges.
- **Ethical hacking courses:** Enrolling in ethical hacking courses helps BISOs understand offensive security techniques and better defend against cyberthreats.
- **Academic programs:** Some universities offer advanced degree programs in information security, cybersecurity, or information assurance, which can provide a solid foundation for the BISO role. While formal degree programs aren't necessarily a requirement of information security and cybersecurity professions, they can prove beneficial in establishing a strong technical and business foundation.
- **Soft skills training:** Coaching in soft skills – such as communication, negotiation, and leadership – can be crucial for success.

Training should align with the BISO's current skillset, areas for improvement, and the specific immediate and strategic needs of the organization. A well-rounded approach that covers technical, managerial, and interpersonal skills serves the dynamic BISO role well. The cybersecurity landscape is constantly evolving, so staying curious and adaptable are key traits for the role of a BISO.

Contributors

Aaron Kirby, Senior Vice President – Security Business Solutions, *Mastercard*

Alok Nigam, Director – Technology Risk & Cybersecurity, *American Express*

Amit Khosla, Business Information Security Officer, *Fannie Mae*

Ann Hines, Business Information Security Officer, *USAA*

Carlos Gonzalez, Business Information Security Officer, *Wells Fargo*

Carly Miller, Business Unit Risk Lead VP, *Comerica*

Donald Schmidt, Business Information Security Officer, *Fannie Mae*

Jocelyn Anderson, Assistant Vice President – Information Security, *HarborOne Bank*

Joseph Millevolte, Business Information Security Officer, *BNP Paribas*

Michael Leking, former Business Information Security Officer, *U.S. Bank*

Nicholas Kelley-Ossey, Business Information Security Officer, *The Travelers Companies*

Segun Yayi, former Business Information Security Officer

Seido Afia, Business Security and Risk Analyst Lead, *Comerica*

Chiheb El Ouekdi, Business Information Security Officer, *Industrielle Alliance, Assurance et services financiers*

Resources

Building Trust

For additional references on the trust equation see:

- https://modelthinkers.com/mental-model/trust-equation
- https://trustedadvisor.com/articles/the-trust-equation-a-primer

Resources regarding the BISO Role

Many resources have been published about the BISO role, including:

- What is the BISO role and is it necessary? | TechTarget
- A new role for the Cybersecurity industry: Business Information Security Officer | GRC World Forums
- Business Information Security Officer Role: 'This Is What I Do' | SecureWorld
- Business Information Security Officer (BISO) Job Description | Jooble
- What is a BISO? Everything you need to know 2022 and 2023 | CyberTalk
- The BISO Role: Where Business Meets Security | IANS Research
- Business Information Security Officer | Cybersecurity Guide

- Cybersecurity Careers: Become a Business Information Security Officer (BISO) | LinkedIn Learning
- Does Your Business Need a BISO | IANS Research

---

[i] https://www.iansresearch.com/resources/all-blogs/post/security-blog/2023/02/21/benchmark-report-preview-the-biso-role-in-numbers