Recommendation on BISO Establishment at Simpton Corp.

EXECUTIVE SUMMARY

The growing complexity of Simpton Corp. and its operations across different regions has resulted in increased security challenges that can compromise sensitive information and assets. Moreover, the variety of regional regulations and compliance potentially put public listing at risk. To enhance data security and regulatory compliance in such a complex environment, I recommend the hiring of Business Information Security Officers (BISOs) to manage and coordinate information security efforts. This report of recommendation provides an overview of the BISO role, discusses the potential benefits and drawbacks of establishing such a position at Simpton, and explains how BISOs could help mitigate upcoming challenges related to the cybersecurity incident. Further, I will recommend how many BISOs to hire and where the positions should be located.

BISO ROLE SUMMARY

The Business Information Security officer is a relatively new role that was established for corporations due to its large scale of operations and/or operating geographies. Let us go into details and have a look at the breakdown of why BISO exists:

1. When an organization is large and spread too thin, BISO is put on top of different verticals and departments to bridge the gaps between business units and Chief Information Security Officer (CISO). BISO acts as a conduit to every one of these business units because the business units can be specialized, apply security differently, and have different security characteristics. This way, CISO has a farther reach because BISOs are concentrating on their respective business unit alone.
2. When an organization has global presents and needs regional specialties, BISOs are assigned to different physical areas to focus on localized security efforts. The role ensures the cybersecurity program for its specific business region is aligned with the company's strategic goals and objectives.

It is common that the larger corporations are also globally enabled, making the decision of hiring BISO even more convincing. BISO and CISO have some duties in common, that is the reason why the industry sometimes refers to BISO as the mini-CISO or deputy CISO. The similarities are there. However, BISO is more specialized and must balance his technical and business roles as opposed to CISO, who is primarily a business leader.

Pros and Cons of BISO at Simpton Corp.

Simpton raised the question of establishing BISOs in specific geographies. It would provide several benefits to do so. First, the new establishment improves oversight of cybersecurity activities and greater alignment with the company's overall strategy. Each BISO can concentrate

on the unique focus for their specific area and receive general directions from the CISO. Secondly, BISOs can achieve readiness for the company's public listing by building relationships with local regulators and stakeholders. The drawbacks of establishing BISO are somewhat incomparable to the benefits it brings. The BISO role is a senior-level position that generates recurring costs. The company should view this as the cost of doing business. Aside from that, there may be potential conflicts between the BISO and existing cybersecurity staff such as the "Head of Security".

Upcoming Challenges and Mitigations

The imminent challenges are regulations. Coming from the European region, Simpton is bound to be responsible for EU's General Data Protection Regulation (GDPR). The US equivalent California Consumer Privacy Act (CCPA) also applies when it comes to the US market. Another challenge is that cultural differences can create difficulties in establishing centralized standards for information security, as the application of these standards may need to be adapted to local contexts.

Simpton needs to be prepared to withstand increased scrutiny and potential legal action related to the breach that occurred in mid-2020. Having BISOs assigned to these two locations would significantly strengthen the security posture and show the general public how sincere Simpton is regarding information security. The BISO establishment provides dedicated cybersecurity resources in specific geographies.

Potential Negative Implications

One of the potential negative implications boils down to decentralization and coordination. When setting corporate policies and standards, it is a challenge for regional BISOs to have a universal understanding and not go off on their own tangent. Another negative implication would be BISOs' areas of specialty could be skewed from one another; one might have a narrow view of what the security requirements are. Additionally, writing an appropriate job description to acquire individuals who can be properly qualified for the job can be a concern.

Recommendation

Based on the potential benefits and drawbacks of establishing BISOs at Simpton Corp., I recommend that the company hire two BISOs. One BISO should be located in Europe, where the company is facing potential legal actions related to the high-profile cyber breach. The other BISO should be in the US, where he focuses on building a robust security program in line with CCPA. I recommend Simpton to centrally recruit from the headquarter and choose candidates from the targeted country or region. It is vital to establish such a role as early as possible. The reason is in a well-established company, it is costly and ineffective to transform and make organizational changes. In the end, it is the practice of making sure that security governance is applied throughout the business, no matter where it exists.

References

Allan Alford on LinkedIn: #ciso #cisos #informationsecurity #cybersecurity #infosec #security #cyber. . . | 56 comments. (n.d.). https://www.linkedin.com/posts/allanalford_ciso-cisos-informationsecurity-activity-6664143871351500800-cKUW/

Irei, A. (2021, June 30). *What is the BISO role and is it necessary?* Security. https://www.techtarget.com/searchsecurity/feature/What-is-the-BISO-role-and-is-it-necessary