Ginger Armbruster, MIPM, Scholarship for Service Student, ISRM

Presented at CISSE, June, 2014

Strategic Planning for a CISO: Strength in Weak Ties

Abstract

Imagine a position that requires accepting responsibility for the behavior of others without the benefit of having direct managerial oversight. Worse, having accepted the responsibility, should anything go awry, the consequences could result in severe financial repercussions, lawsuits and media exposure - in other words, a position with all of the potential downside and little control. Such is the case of the Chief Information Security Officer, or CISO, especially in the private sector which owns 85% of critical infrastructure.

As companies increasingly rate information as their most valuable asset, the executive in charge of maintaining the integrity and security of those assets has become the focal point for security problems in large and complex enterprise environments. Establishing the policies, procedures and training centering on data and system security across multiple departments requires unique consensus building skills and engendering trust partnerships across a complex range of corporate dynamics. And yet, in a crisis involving the loss of vital data, inadvertent disclosure of private information or malicious disruption of systems from outside bad actors, the CISO is in the hot seat. Often, the CISO office has minimum staff and maximum exposure.

*This paper presents an analysis of the strengths, weaknesses, opportunities and challenges of the CISO for a large state university that can provide insight into the larger problem faced by the private sector.. The purpose is to illuminate the management issues facing the executive responsible for promoting the mission of the office—a mission to provide policy and guidance tow*ard *maintaining a secure computing environment.*

1. Introduction

An analysis of the CISO role begins with an acknowledgement of two major challenges. The first is that risk management as it pertains to computing and data is a moving target. There is a constant flow of new technologies, requirements and end-users into the University. This creates an environment that is impossible to secure from all present and future risks to information systems. Given this reality, the CISO's objective is not to dictate initiatives to eliminate risk, but rather to provide information and support to assist executives within the University organizations to do their own risk management due diligence. Second, the Office does not have responsibility for the equipment or systems at risk, nor can it enforce its recommendations. It can only delegate and suggest better methods and procedures in the face of almost assured breach incidents of sensitive data and systems.

While strategic planning and analyses of strengths, weaknesses, opportunities, and threats (SWOT), are increasingly commonplace in the planning and budgeting of critical infrastructure systems, we present this case as one in perhaps a series for the purpose of developing discourse on the politics and economics of organizing to manage cybersecurity. That is, one can perform a SWOT analysis on a system, and one can perform a SWOT analysis of the organization charged with managing the system. We believe that many outstanding issues in cybersecurity exist because of under-analyzed, and coincidentally weak connections, between the political-economic dynamics of organizations responsible for technical systems.

The following case illustrates relationships that capitalize on the strength of weak ties (Granovetter, 1973) between a CISO and fellow administrators from disparate parts of a large and technologically active public University.

Through a series of six interviews with the CISO and key university stakeholders, we gathered the necessary information to review the strengths, weaknesses, opportunities and threats (or challenges) facing the office in accomplishing their mission. These interviews were with the following University positions:

- The Chief Information Security officer
- Deputy Chief Information Security Officer
- VP of Advancement
- Executive Director of Risk Management
- Director Lab Services

The process of analysis included the steps outlines in Eugene Bardach's book, *A Practical Guide For Policy Analysis: The Eightfold Path To More Effective Problem Solving* (2004).

The paper outlines, briefly, the threat landscape experienced at the University. This is followed by an overview of the strategic planning process in the CISO offices, an analysis of stakeholders, and a SWOT analysis. So that the subjects of this study may remain anonymous, we have condensed our business analysis into a brief summary, followed by an outline for screening new business opportunities, and a set of "big" questions that, from the point of view of participants in our research, currently govern decision-making for the CISO.

2. The Threat Landscape

In this case, the CISO Office reports through the IT department with funding directly from the Provost (a position similar to a chief operations officer). The unique activities of the CISO office provide opportunities for privacy and audit investigations that could compromise funding and invite potential by allowing for a conflict of interests. For this reason, according to the CISO during our interviews, only two individuals are in the position to fire him from his position.

Maintaining computer security in a large university computing system includes oversight and support of both the physical and virtual environment. The following are included in the threat landscape that the CISO office is tasked with managing:

- Intentional damage or unauthorized access to physical systems and data centers
- Phishing attacks and delivery of malware through email attacks
- Cyber stalking and harassment of employees and students
- Targets that include:
  - PII of employees and students in a community of over 30,000 individuals
  - Healthcare records of hospital and clinic patients
  - Intellectual property and research across all academic disciplines, including regional and Federal government and military joint projects
- Human Resources
- Grading and academic records
- This university as an ISP provides a regional Internet connection, making it a target for commercial and hostile nation-state criminal activities

3. Strategic Planning at a University CISO

The strategic planning process for the CISO office begins with a semi-annual survey that is distributed to the University's Security Council – whose membership spans many divisions of the University. This document, while not shared outside of the Council, seeks to collect information about the effectiveness of

the current initiatives and suggestions for future directions. According to interview subjects from Security Council member offices, the planning agenda includes the crucial topic of current threats and risks. These immediate concerns inform the strategic direction for the Security Council augmented and shaped by the CISO's global perspective. Responses vary depending on the areas of interest of the members who answer.

The strategic planning process requires networking among many diverse organizations with missions ranging from fundraising to medical patient care. As already emphasized, the CISO Office does not seek to enforce risk management initiatives, but rather provides leadership and support for optimizing policies and procedures to minimize risk with the use of computing technologies. For these reasons, strategic planning is both an event with a documented output and an on-going process of information exchange. A large part of the strategy planning process is done by building consensus during informal meetings and discussions. As one interview subject stated," the success of the office is not about enforcing compliance, but about building trust."

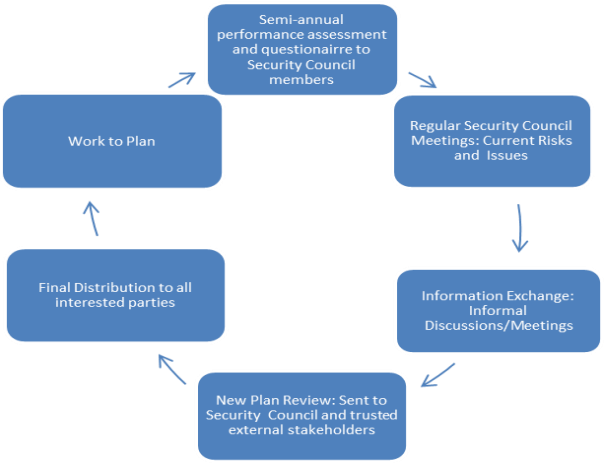

Figure 1. The Strategic Planning Process

3.1. Analysis of Stakeholders

The CISO's Office is the nexus for leadership, education and support for risk management initiatives pertaining to a wide range of data storage and computing technologies for University departments, offices, and affiliates. As the CISO Office provides oversight to a broad range of topics pertaining to risk management, the stakeholders interested in its strategic planning process are numerous. Below is a graphic representation of stakeholders in the strategic planning process for the Office of CISO:

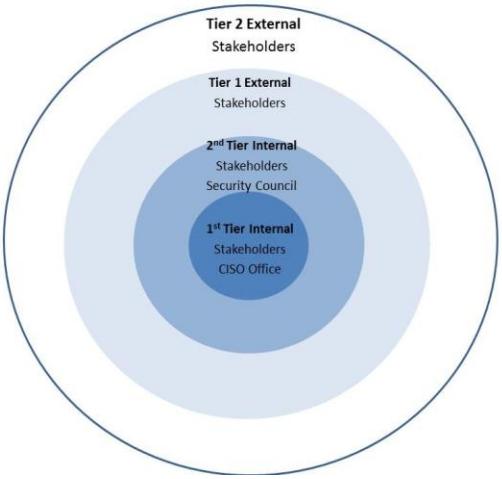

Figure 2. Office of CISO at the University: Stakeholder Map

Tier 1 Internal Stakeholders - The center of Diagram 1 contains the direct employees of the office. The roles of these professionals are taken from the organizational chart posted on the website:

- CISO
- Associate CISO
- Asst. Director of Security Services
- Sr. Security Advisor
- Lead Security Engineer
- Network Security Specialist
- Asst. Director of Privacy
- Security & Privacy Learning Specialist
- Information Assurance Architect

These employees, including the CISO, have direct responsibility for the success of the strategic planning process and the daily work product of their role or function. The strategic planning process defines and refines their functional roles and assists in the identification and allocation of priorities and funding. As a customer service-oriented department, the CISO Office uses planning as an opportunity to provide guidance and to ensure that pertinent University risk management issues are addressed and staffed.

Tier 2 Internal Stakeholders - The second tier of internal stakeholders is a variable group taken from upper management positions from the four core functions of the University: Education, Research, Healthcare and Athletics. All members play an active role in determining the content of the strategic plan. Membership of the Council is variable and reevaluated on a periodic basis to ensure that all University interests are appropriately represented.

Tier 1 External Stakeholders - Tier 1 External Stakeholders include those entities that have direct regulatory oversight of operations or financial involvement with the University. They have interest in the functions and operations of the CISO Office, but are not involved in developing the strategic plan. Performance is assessed or commented upon, but discussion about allocation of resources or prioritization of initiatives is not within the scope of their interest or involvement.

Tier 2 External Stakeholders - Tier 2 External Stakeholders are agencies that are affiliated with the University, such as a local Hospital for children, another area hospital, health clinics in the area, remote

campus locations and finally local trusted CISOs from other organizations who provide support and assistance. These organizations have their own CISO offices but rely on a two-way information flow to maintain consistency and currency with risk management issues.

An analysis of stakeholder participation in the strategic planning process is somewhat complicated by the fact that involvement is often based upon criteria important to their specific business interests. A more appropriate analysis would look at stakeholder interest in the various topic areas covered by the CISO's Office. A graphic representation of stakeholder's role in influencing and supporting the strategic planning process is shown below:

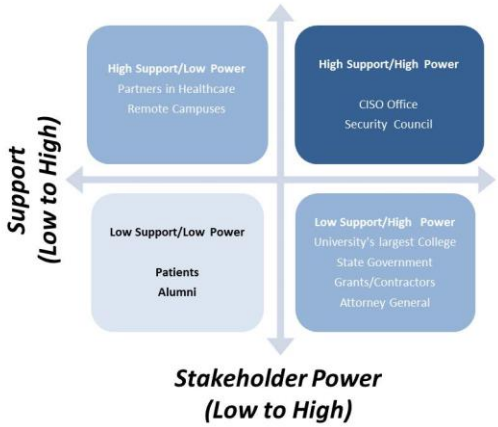

Figure 3. Stakeholder Support/Power Matrix

.

This mission statement speaks to the oversight role the CISO plays in providing information that is useful to the risk management "customers" they serve across the University. It is effective for three reasons:

1. **Consensus Building**: It does not explicitly address the perceived leadership role or the global context the Office provides regarding specific risk issues. This choice of wording deflects any perception of directive behavior. The success of the CISO's role relies both on building consensus and empowering individual professionals to lead their own risk management initiatives – in effect, leading from behind.

2. **Reduced Scope of Responsibility**: If the mission statement took a more directive approach, the Office would be both tacitly and explicitly accepting responsibility for a much larger scope of work than its staffing and funding can embrace. Additionally, the Office would be accepting more direct responsibility for both auditable and regulatory compliance.

3. **Issue-less**: This mission statement avoids calling out any one area of technology or issue that might create concern or conflict for stakeholders. By not using words such as "mitigate", "due diligence" or "technology" it avoids creating tension with those who seek to advance more or less aggressive technologically forward agenda with less reference to risk management, for example.

In our analysis, we noticed that the mission statement addresses the role of the department in a non-confrontational and generalized way. Should the Office objectives change from providing customer service, information dissemination, and consensus building around risk management, to more ownership of the issues across the University landscape, then consideration of more proactive and directive language would be appropriate.

4. SWOT Analysis

Analysis of the internal strengths, internal weaknesses, external opportunities, and external threats (or challenges) follows, accompanied by tables in appendices A-D. This work was guided and framed with reference to Bryson and Alston's (2004) guidebook for strategic planning.

Strengths - In reviewing environment in which the CISO Office runs, we begin with a review of the internal strengths of the office. Appendix A suggests that the office's strengths may be represented in six categories. First, the office works on a single mandate. The CISO is able to focus on risk management exclusively, rather than as an adjunct to a larger Information Technology mission. The sole focus is supporting the varied aspects of assuring the integrity of information and data across the various technologies in the University environment.

The CISO office is staffed with experienced and respected professionals, including the leadership of the office. This team offers a varied and complementary set of technical and communications skills, preparing them for the changing variety of issues that arise. In interviews, the CISO confirmed that the most important asset any member of the office can offer is a well-connected network representing professionals who respect and work well with customers and staff. This is especially important at the leadership level of the office. The CISO staff has cultivated a well-earned reputation for trustworthiness that creates an atmosphere conducive to building and maintaining an effective collation.

Finally, the office has effectively implemented a website and various tools for monitoring and communicating their activities in a highly visible and effective manner. One of these is the development of a tool, which the CISO describes as one of "the most revolutionary opportunities we have" to provide a visual representation of databases, administrators and other aspects of the University information flow. This tool is an important management tool for the overall infrastructure of the office. This includes location, access, clearances, and credentials. This works in conjunction with the coalition that the office has built among the important internal and external stakeholders.

Weaknesses - The Office's potential weaknesses are fivefold. First, there are limitations in having a small staff. The CISO stated that 10 people support the University, a large state employer and he compared this to an office at a banking interest with a staff of 150 people supporting a system a fraction of this size. The size of the staff creates a need to limit and prioritize projects and initiatives and to utilize an effective strategic methodology. One means of overcoming this limitation is to use outside resources and to share "in kind" services within the larger area CISO community. Example of this is a recent sharing of training materials with area hospitals and the use of the Attorney General as legal counsel as needed.

Further, the scope of the office is curtailed by the lack of direct management and responsibility of the office. Providing information and oversight limits the CISO's ability to ensure that appropriate programs and directives are instituted.

A further potential weakness of the office is a result of the internal management structure which puts the CISO Office under the auspices of the IT department. This creates an inherent tension between supporting new technologies and implementing appropriate and effective risk management policies and procedures.

Finally, the customer service aspects of the office create a limitation in mandating initiatives or programs that would support compliance or important aspects of risk management in support of the office's mission statement. These features are listed in Appendix B.

Opportunities - Risk management is currently important at the highest level of the United States government as an important aspect of combating cyber terrorism. This presents opportunities to the CISO Office for funding and collaboration at the State, and Federal Government agency level. As funding to higher education becomes less abundant, this may provide a way to offset budget cuts and limitations.

The broad support base that the CISO team has created through effective relationship and consensus building may be helpful in maintaining support across the University and alliance agencies. The Office is not dependent on any one decision maker or funding source should political interests and alliances shift.

Finally, the dynamic risk environment provides a constant injection of new issues and risks to make the office a vibrant and essential agency. To protect the anonymity of our case subjects, the details of opportunities have been removed from Appendix C.

Threats - Threats to the CISO Office are derived primarily from nature of the business conducted by the office, and current funding concerns. The CISO Office is dependent on its customers to successfully implement programs and initiatives. The office's effectiveness is determined not necessarily by their direct action but how successful they are in supporting and influencing others in managing risk issues in their office environments. This is compounded by the nature of information security threats that create a high visibility environment for failure. Without direct responsibility for the potentially dire results of inaction or failure to succeed in implementing appropriate programs, the CISO and staff are unable to direct their own destiny and their performance will be determined tangentially.

The changing landscape, churn of issues and concerns creates a need for the office to maintain high agility to meet potential customer requirements. As a customer service organization the office must direct the risk management agenda but also answer customer requests and needs.

Finally, the current recession and state funding reductions have resulted in University-wide budget cuts that affect all departments, including the CISO office. There has been a consistent decrease in funding of more than 2 percent annually to the CISO Office, which reflects the overall decrease in the University's entire operating budget, while the need for support and services from the CISO Office has increased.

5. Business Analysis

The CISO Office business model is a customer-service oriented, internally-funded University oversight office which provides a broad base of support and information for risk management issues. The Office offers leadership in incorporating risk management technologies, policies and practices into all aspects of University's operations. These are primarily consultant and educational services and support for initiatives and programs implemented by the agencies the Office supports**.**

The CISO Office was initially funded by the Office of the Provost, for the purposes of setting up the office and initiating the first round of staff hiring. This funding has remained the primary funding source, and remains an annual budget line item. As the office has experienced an annual budget cuts over the past two years, these potential revenue sources may become important options.

Risk management is a very current topic and will continue to be current as cyber threats to information and computers continue to provide every-changing challenges to organizations and businesses reliant on technology. This trend takes on a greater currency as the Federal Government remains focused on threats to our critical infrastructures (including computing and information systems) from both inside and outside terrorist organizations. This has resulted in an increase in government funding for offices and agencies which are on the forefront of discovering and combating these threats. Funding has been available for education, mitigation, research and other programs to combat potential threats.

It is possible to consider that there are several possible alternatives to this internal University resource: outside consultants, the State CISO office, and the IT department. None of these "competitive" alternatives to the current CISO office are optimal. In fact, the reason for the CISO Office and CISO function is that risk management is its own discipline requiring a level of internal organizational understanding and consensus building that is impossible to achieve externally though either consulting services or outside agency support.

6. Screening New Strategies

We identified the following criteria for the CISO Office's Strategy Screen. Though currently done as an "intuitive" part of the planning process, the interviewees all found it interesting and informative to go through the exercise of formally articulating these criteria:

Is it consistent with our mission? This question asks if a new strategic initiative or implementation fits within the scope and overall strategic direction of the office. An endeavor or proposal that departs from the stated direction of the office would require support and consensus of all internal and external stakeholders in order to be successfully adopted and implemented.

Does it build on or reinforce or current competitive advantage(s)? While the CISO Office does not consider that they have direct competitors for the services and support they provide, any strategic options should be explored as alternatives that are unique to the CISO function.

Will it fit within our budget constraints and is it cost-effective? Any new initiatives should be explored in the context of the current budgetary environment. Cost-effectiveness requires further definition, as risks must be identified and quantified for each new technology or initiative along with implementation and on-going costs of the system or program, deployment and any training required. An example of this cost-effectiveness equation is the implementation of a software package that costs $10K. A code review (to assess risk profile of the software) that would cost $150K to complete must be weighed against the potential cost of a data or systems breach. For a system or program that exposes $4-5M worth of data assets a code review must be carefully considered, while a system with a lower exposure profile might result in a different assessment.

Does it build on our leadership position in the community? Maintaining the Office's leadership position within the CISO community and the University environment at large is an integral part of the office mission. This includes a perception of leadership with the State's governing board for the University and other members of the executive management team. An additional consideration here is whether the initiative will continue to support and foster future CISO leadership - the next generation that will be tasked with implementing a risk management agenda at the University.

Is it acceptable to PASS Council membership and builds on our consensus? New strategic initiatives must have the consensus of the Security Council membership and promote or support individual strategic plans for Security Council members. An important aspect of this consideration is that the Office must be focused on the priority projects and concerns of the Council membership.

Is it consistent with strategies within the alliance? Consistency with CISO offices throughout the alliance community is an important part of promoting good risk management hygiene and furthering the overall goals and objectives of the risk management discipline.

Is the proposed strategy scalable? The question of scalability is complicated by the fact that there are many different environments within the Office's scope of practice. Some initiatives will not transfer outside of confidential or privacy law compliance areas, for example, but should at least be available to a broad group within specific areas of implementation.

Is it consistent with other tool sets or systems already deployed? Though the CISO Office does not physically support the technical aspects of the systems and programs that are deployed throughout the University, they must be aware of compatibility, and feasibility of any program or system they promote or support to work within the current systems architecture.

Is it possible to track and monitor progress? Because the office is not directly responsible for the implementation of systems and programs, there must be a way to monitor and quantify progress and success or failure of an initiative. As the Risk Management Director stated, "If it cannot be measured, what validity does it have in this context?**"**

Does it meet the full threat spectrum, including threats to classified systems and data? There is another side to the CISO office mission, and that is to support classified data, systems and research that are conducted on campus and by University affiliates and alliance members. Any new initiatives must take into account potential impacts on or risk to these systems, even if they are not directly in the purview of these projects.

Does it foster a culture of security on campus? One aspect of the CISO job description is to "foster a culture of security on campus." This includes fostering a sense of trust with a broad range of academic and research environments with an equally diverse range of political and social perspectives. This translates to a need for the CISO Office to be aware of the potential perception that individual members of

the University community may have about aspects of security and risk management programs and systems. He emphasized the need to maintain a "soft bunny" look and feel to the real world risk mitigation measures that he spearheads or supports. This could also extend to sensitivity about financial and collaborative efforts with government, private industry and between departments and groups in the campus community.

7. Asking the Big Questions

Through the interview process, we confirmed seven strategic issues that could be considered "Big Questions" for the CISO Office. These are the questions and concerns that relate most to the continued success of the office. The purpose of posing these is to investigate the options and viability of the office in setting direction as a leader in information security.

1. How to address current and future funding challenges?
2. How to retain and nurture key staff in a tight budget environment?
3. How to maintain and increase the leadership position in the University and larger CISO community?
4. How to meet and address the risk impact of the introduction of new technologies to the University environment?
5. Can the CISO Office function as an independent auditing entity within current management structure under the IT Department hierarchy?
6. How to communicate complicated information assurance issues to the general "audience?"
7. Are we addressing the top priorities for the University and Security Council?

8. Implications and Conclusions

As an overlay office providing services across the University landscape in a volatile and highly visible arena, this office is tasked with a huge and ever-changing scope of responsibility. Changes to its strategic plan have wide-reaching implications and require a level of personal and concentrated consensus building on the part of the Office's leadership that could easily go awry in less deft and experienced hands.

In our final interview, the CISO spoke about the Big Question that really keeps him up at night – how to cultivate the next generation of leadership to ensure the continuation of the kind of networking and personal relationship building that has made this office so successful to date. He went on to discuss the ramifications of the kind of power this office can wield in shaping and supporting a culture of information assurance – including the processes and people that are necessary for the ultimate success of the effort. He pointed out that he has a shelf in his office of over 6,000 business cards that he has collected in the past 10 years that represent not just people he has met, but personal contacts he has made over meals and coffee in order to add to his functional professional network. It takes years to build this level of community involvement and it not easily transferable to others who may follow him in his CISO role.

We believe two frameworks assist in understanding the role of the CISO and, for this case study, the success this CISO has had with such limited resources and authority in serving the needs of a large, technologically dynamic organization. The first of these is an insurance model of CISO service. The second is the idea, from Granovetter (1973), that the strength of weak social ties between individuals across organizations may allow networks to perform as well as (or perhaps better than) their hierarchical or contractual counterparts.

The conundrum of the office of CISO is that if it is done correctly, the true value of the work done is difficult to value. It is in the event that security and privacy policies fail or absent that the value of the office's work may be derived. In this way the CISO role is not unlike the insurance industry. However, because computer and data security and the impact of failure of these systems to protect secure and private information is still a relatively new area of thinking, there is a paucity of actuarial table type data to draw upon to place value.

Because of this, the CISO must build trust and educate their customers about the kind of damage and costs that may be incurred in the event of a data breach. CISO's must build relationships over time to ensure that the information they provide is relevant and helpful. They cannot mandate the adoption of security policy as much as provide information and lead by example. Becoming the Department of "No" or attempting a punitive approach to education will not result in strong relationships based on mutual trust that are so necessary for the office to be successful.

9. References

[1] Bryson, John and Farnum Alston. *Creating and Implementing Your Strategic Plan: A Workbook for Public and Nonprofit Organizations*. New York: John Wiley & Sons, 2004

[2] La Piana, David. *The Nonprofit Strategy Revolution: Real-Time Strategic Planning in a Rapid-Response World*, Fieldstone Alliance Publishing, 2008.

[3] Bardach, Eugene. *A Practical Guide For Policy Analysis: The Eightfold Path To More Effective Problem Solving*. CQ Press, 2004.