Searching for the Right Fit

Balancing IT Security Management Model Trade-Offs

IT security professionals' effectiveness in an organization is influenced not only by how usable their security management tools are but also by how well the organization's security management model (SMM) fits. Finding the right SMM is critical but can be challenging — trade-offs are inherent to each approach but their implications aren't always clear. The authors present a case study of one academic institution that created a centralized security team but disbanded it in favor of a more distributed approach three years later. They contrast these experiences with expectations from industry standards.

Kirstie Hawkey,
Kasia Muldner,
and Konstantin Beznosov
University of British Columbia

The critical challenge of protecting an organization's assets from Internet attacks is multidimensional. Success depends not only on the usability of security management tools but also on the overall effectiveness of processes for IT security management. Many factors influence these processes, including an organization's level of commitment to security[1] and the type of security management model (SMM) that shapes the security team's structure, dynamics, and responsibilities.

What's more, the recent push toward accountable IT governance has highlighted the need for formalized IT security management structures that can meet legislated requirements. For example, the Sarbanes-Oxley Act of 2002 mandates accountable use of IT controls in publicly traded US companies. However, legislation and guidelines for IT governance (such as the IT Governance Institute's "COBIT: Control Objectives of Information and Related Technology"; www.isaca.org/cobit.htm) have focused on general IT management, without taking IT security specifics into account.[2] Notable exceptions are security standards and guidelines from organizations such as the International Standards Organization/International Electrotechnical Commission (ISO/IEC)[3] and CERT.[4]

The CERT handbook for security incident response[4] presents several SMMs and lists factors that organizations should take into account when choosing one, including the organization's size, security services, available resources, and organizational unit in which IT security professionals are embedded.

1089-7801/08/$25.00 © 2008 IEEE

The CERT handbook is intended to serve as a guide for establishing and improving IT security management processes, but its authors propose supplementing the information with data from other organizations' real-world experiences with various SMMs: "one of the most beneficial steps a newly forming team can take is to seek opportunities to meet other teams."[4] Unfortunately, obtaining this information can be difficult due to the information's sensitivity. Furthermore, IT staff in general, and security practitioners in particular, are chronically overworked and might perceive invitations to share their experience as an additional uncompensated burden.[5]

Despite these challenges, we conducted 34 in situ interviews with 36 IT professionals from various organizations as part of the University of British Columbia's HOT Admin research project (www.hotadmin.org), which investigates human, organizational, and technological aspects impacting security practitioners.[5] Here, we present a case study using data from 10 of those interviews, which we carried out in one educational organization. This organization established a central security management office and then disbanded it three years later in favor of a decentralized approach.

One Organization's Experience

Our case institution is a large, distributed, Anonymous Academic Organization (AAO) that includes in its central administrative core a Central IT department. AAO comprises more than two dozen decentralized units, including faculties, schools, research institutions, and departments. Central IT provides support to the organization that includes the IT infrastructure and security. All case study participants devoted at least some of their time specifically to security. Figure 1 shows the organizational structure, distribution of participants across the organization, and classification of participants' positions.

AAO faces numerous security-related challenges, due in part to its academic nature — specifically, its openness. This not only makes policy enforcement difficult, it also means that accessibility and information sharing is encouraged. Security practitioners must protect private and confidential information, educational and research labs, and individual machines. A second security challenge our participants mentioned is the organization's diversity and decentralized structure, a characteristic many institutions share today. AAO's organizational units vary with respect to size, the degree of resources available for IT security, and the set of activities a particular unit needs to support. This diversity makes it hard to have consistent security policies across different parts of the organization. Furthermore, communication across the distributed organizational units, each with their own structure and subculture, can be difficult.

To address these security-related challenges, AAO has undergone several reshuffles with respect to its security team. Let's examine its experiences as it transitioned between IT SMMs. (A detailed account, including participant quotes, is available elsewhere.[6])

Forming a Centralized Security Team

Until a few years ago, AAO had no formal IT security team, although several IT staff within Central IT were security minded, forming a loose team that performed some security responsibilities and received security training. This team met on an informal basis and discussed various security issues and projects. Some AAO managers periodically attended these meetings and would attempt to find funding and resources to implement any security-related projects discussed. This team appears to have limited its discussions to issues and projects under Central IT.

To move toward a formal cooperative management model, AAO formed a centralized security office in 2003 that consisted of a security manager hired into that role and three dedicated security professionals. Two team members were technically inclined, and one had extensive experience administering the organization's responsible-use policy. The security office served the greater organization as well as the Central IT department and was responsible for security and project oversight within Central IT. Although it had a broad mandate to ensure AAO's security, the central security office had no direct authority or control over the end users within the organization's decentralized units.

AAO chose a centralized SMM to promote effective security practices and communication, deemed necessary for a large, decentralized organization in which the security team lacked authority over the distributed units. Security team members anticipated that in addition to facilitating communication and promotion, the creation of the security office would have several other benefits. With a manager and a security budget,

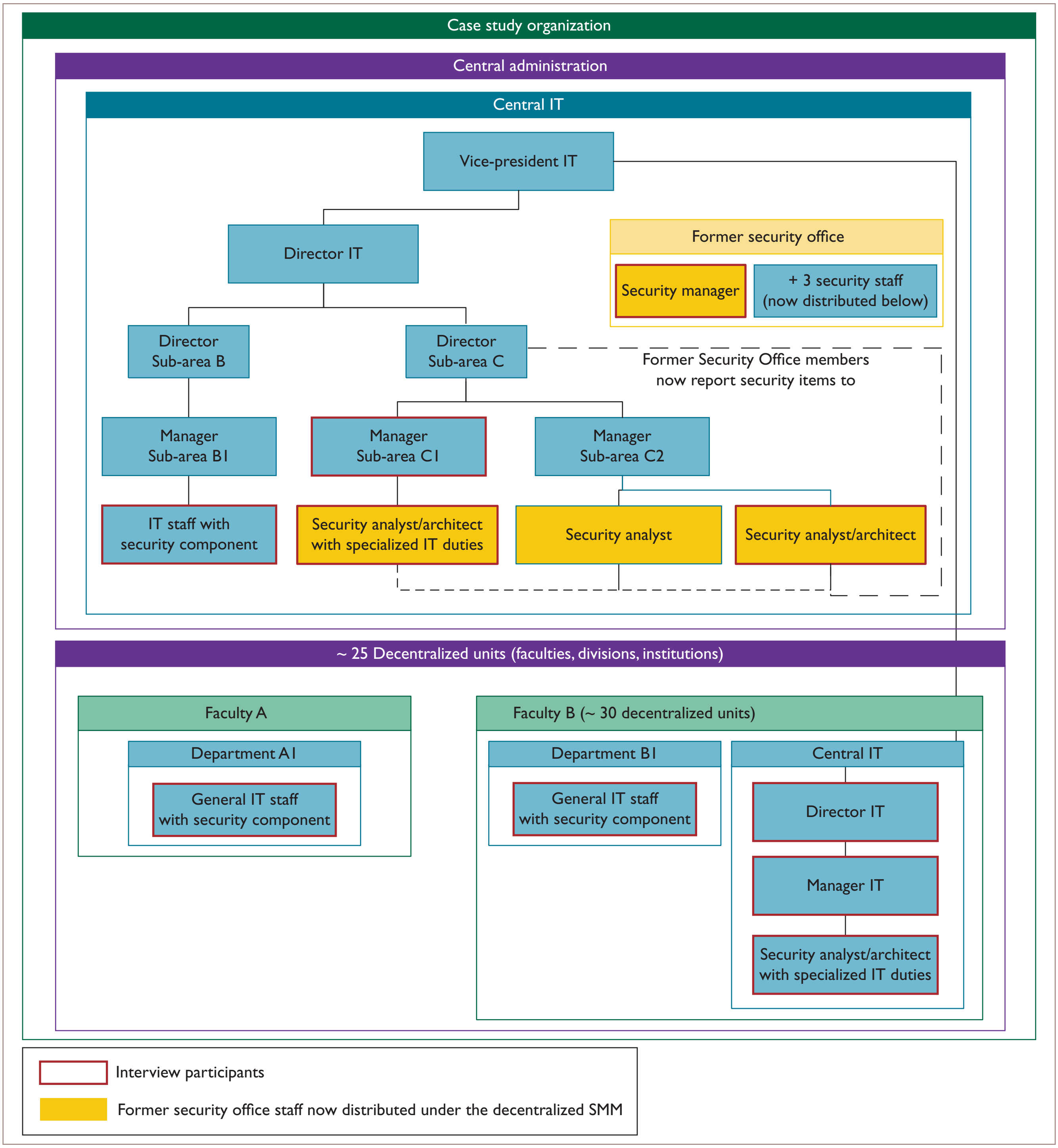
Case study organization
Central administration
Central IT
Vice-president IT
Director IT
Former security office
Security manager
+ 3 security staff (now distributed below)
Director Sub-area B
Director Sub-area C
Former Security Office members now report security items to
Manager Sub-area B1
Manager Sub-area C1
Manager Sub-area C2
IT staff with security component
Security analyst/architect with specialized IT duties
Security analyst
Security analyst/architect
~ 25 Decentralized units (faculties, divisions, institutions)
Faculty A
Department A1
General IT staff with security component
Faculty B (~ 30 decentralized units)
Department B1
General IT staff with security component
Central IT
Director IT
Manager IT
Security analyst/architect with specialized IT duties
Interview participants
Former security office staff now distributed under the decentralized SMM

Figure 1. The Anonymous Academic Organization (AAO). Participants were distributed across AAO and held various positions.

they wouldn't have to fight for resources, and they wouldn't need to convince others (at least within their security team) of security's importance. Indeed, AAO recognized security to be a rapidly evolving concern, and the security office members received a training budget higher than the standard 5 percent given to Central IT. However, the security group also anticipated challenges with trying to balance the potential of new IT security projects with a lack of experience across both the organization and Central IT.

The strongest benefit to having a central security office might be that it provides a well-established single point of contact for security-related communications. To improve collegial relationships and encourage security awareness across the organization, the security team tried to be accessible. They saw communication as integral to being security professionals and, as such, were open to receiving phone calls and emails. They didn't find this level of availability to be disruptive because they didn't have much operational responsibility, which they in turn viewed as strengthening security within the organization. Although security team members weren't necessarily responsible for operational security, while the central security office existed, their activities included implementing VPNs and firewalls.

One key aspect of the organization's IT security governance strategy was to embed security into the project- and change-management processes. The security group conducted formal reviews and signed off on projects during both the design and implementation phases. During the design phase, they reviewed plans to ensure that the plan had taken security into consideration. On large projects, they worked with IT auditors from the organization's internal audit department to draft formal recommendations about IT security. Prior to a system going live, they conducted a security review, including vulnerability scans. Any changes to production systems within Central IT were presented to the change approval board at a weekly meeting. The security team played a key role in these meetings and held veto power over changes that could compromise security.

In addition to security assessments, the security office was responsible for security oversight for the organization and for developing and enforcing security policies. The central security office used a split security model of awareness and enforcement. The security manager took on the security awareness and advice function within the organization, whereas the internal audit department handled enforcement.

The central security team also took responsibility for triaging security incidents. The organizational stakeholders would notify the security team via phone calls and emails. Additionally, the team received tool alerts. One advantage of centralization was that the security team members could take a proactive approach to such incidents, maintaining an overview of security vulnerabilities for the organization. Not having operational tasks gave them time to learn about new vulnerabilities, develop scripting tools to check for signs of exploits, scan systems in both Central IT and the overall organization for problems, and assess problems found. However, the security office didn't generally fix the affected systems, but rather forwarded the information to IT staff in the corresponding departments — that is, the "owners" of the systems.

At least half its team members viewed the centralized SMM as successful. Indeed, some of the central security office's initiatives are evident in processes still in place today. For example, the security review during system design phases and the procedures for security incident response haven't changed since the group's dissolution. However, the central security group wasn't as successful at creating security policies. One participant recounted how the policies didn't have the reception they expected from the organization, and the project was dropped. This participant thought that the management within Central IT didn't view the policies to be as "sexy" a concept as the firewalls the IT staff were installing throughout the organization.

A Shift to Decentralization

AAO disbanded the central security office after roughly three years. Although we didn't interview the manager who made the official decision, our interviews with other stakeholders suggest that several factors led to the disbanding. One perception was that security was too divorced from operations with a centralized SMM. One of the three security professionals within Central IT was frustrated to be uninvolved in implementing IT security controls and actively lobbied for a more operational role — without such a role, the security office was limited to giving only recommendations, relying on other specialists within the IT organization to reconfigure affected devices and systems. However, the "operations" people had their own responsibilities and so often resisted taking on security-related tasks. This particular participant was unsure of all the factors that influenced the security office's dissolution, but perceived that it might have stayed if the security group could have imposed recommendations. For this participant, a move to a decentralized SMM was necessary given the lack of authority across the distributed organization. Another participant echoed the perception that security should be embedded within the organization because it's integral to IT, describing security as a band throughout all aspects of AAO.

Interestingly, the decentralized security office has lacked a security manager since the original manager received a promotion roughly a year ago. Although some support within Central IT still exists for having a security manager, the position has yet to be filled. The other three security practitioners are now distributed between two of the Central IT groups and are still the only three within Central IT whose main focus is security. Their responsibilities under this decentralized SMM include security tasks such as policy development, reviewing new system designs, participating in change management, responding to emails and alerts, checking logs to look for possible intrusions, and responding to threats and incidents, as well as more operational tasks such as network security appliance maintenance, centralized firewall management, and standard network administration.

These three members of the former security office still function as a cohesive group in many ways, despite lacking a formalized structure. The general contact email address (security@...) and phone number for the former security office are still active, for example, and the former group members still handle email triage, relying on transactive memory[7] to judge who will pick up certain items on this and other email lists that they monitor.

These members currently meet with each other for two to three hours every two weeks to "talk about policy, new threats, new things, what tools we are using, basically how to manage all the flow of information we are getting all the time." This group's reporting structure is also in transition and quite informal. Currently, a Central IT director has taken on some security-related management duties, including keeping abreast of and prioritizing the main security actions.

Policy creation appears to be going well under this decentralized model, although the success is likely less due to the SMM than to the external forces driving policy development. AAO currently must draft and implement internal security policies for servers and workstations to comply with the Payment Card Industry requirements, so policy development has become a high organizational priority. One of the former security office members leads the policy committee, which was to include managers and other representatives from the affected groups. However, a lack of managerial participation has made iterating policy drafts difficult for the committee; the IT and security staff present in the meetings can describe usual practice, risks, and procedures to mitigate the risks, but managers and senior managers must actually set the policy and approve the budget for the necessary infrastructure.

The new, decentralized SMM appears to deal with security incident response the same way as under the centralized SMM. One participant stated that the decentralized SMM didn't influence security incident response either way "because all the people that need to communicate with each other were doing so." The distributed security group members still have the primary role of determining whether a potential incident needs to be investigated and forwarding any problems to the appropriate administrator within Central IT or across the organization for investigation and resolution. One downside to decentralization is that the lack of a security manager and enforceable security policies means that the informal group must sometimes escalate their security incident responses to somebody with the ability to enforce their request for action.

One intended benefit to distributing security members into Central IT's subgroups was to increase security awareness within those groups, which appears to have happened, at least for those two groups with distributed security team members. Moreover, the distribution helps the IT security staff know what's going on within Central IT's subgroups. However, the practitioners' operational tasks leave less time for overseeing the whole campus, so overall awareness of security within the organization might have declined. Although at least one security practitioner is still actively trying to maintain an overview, this participant also expressed some frustration at the lack of cooperation for this across the organization. This same participant expressed concern at having insufficient time to keep abreast of the latest vulnerabilities.

Case Study Experiences vs. CERT Guidelines

Although guidelines (such as the CERT handbook[4]) do help practitioners and managers consider the various SMM trade-offs when establishing a security team within an organization, they also stress that choosing an SMM is not cut-and-dried for three key reasons.

First, because each SMM has specific strengths and weaknesses, choosing a model entails making trade-offs. However, as the CERT guidelines acknowledge,[4] doing so isn't straightforward because those trade-offs' implications aren't immediately clear. Let's look at the development of expertise within a security team, for example. A decentralized model encourages security team members to gain operational expertise via day to day operations but also leaves little time for them to learn about new technologies and vulnerabilities, which a centralized model does support.

Second, the CERT guidelines are fairly general in terms of how organizational characteristics impact a given SMM's applicability. For instance, the CERT handbook specifies that a centralized model is appropriate for small organizations or large distributed organizations, such as educational ones, whose organizational departments or units share common characteristics. What's unclear, however, is what these common characteristics are and how they impact an SMM's suitability.

Third, although CERT guidelines specify that an SMM should meet certain requirements, organizations might not be able to implement security teams precisely as described, further complicating the question of which SMM to choose. Our case study illustrates the difficulties that can arise when an organization doesn't meet its SMM's underlying assumptions. The CERT handbook specifies that the security team in a centralized model should have authority over the organization (to enforce recovery and mitigation strategies after a security incident, for example). However, AAO's academic nature meant that the security team had "no teeth," so it could not enforce some security processes, particularly in the distributed organizational units outside Central IT.

These challenges mean that a given model's expected benefits and drawbacks might not be realized in practice. To see the extent to which this occurred for our case study, we compared AAO's experience with expectations outlined in the CERT guidelines with respect to how each SMM influenced various aspects, including consistency, responsiveness, and expertise. As the sidebar shows, in some instances, mismatches occurred between expected SMM characteristics and reality. Although some discrepancies weren't surprising — given that AAO deviated from the idealistic CERT model — others were unexpected.

Centralized Model in Practice: Benefits and Drawbacks

AAO based its initial move to a centralized model on efforts to promote security and encourage communications with various stakeholders. Both efforts were deemed necessary for effective security management in a decentralized organization in which the central security group doesn't have much authority or control over department end users. AAO expected communication and promotion to be strengths under this SMM, as compared to, for instance, a decentralized model from the CERT guidelines For AAO, a centralized SMM did indeed realize strong communication and promotion of security, which is consistent with the guidelines.

The centralized model offered other expected advantages that our case study participants didn't discuss but that might interest others trying to choose an SMM. For example, a centralized model allows an organization to hire dedicated professionals with greater expertise in security. In our case study, all participants were already working within the organization at the time the centralized office was formed, so we don't have data on how the SMM influenced hiring practices.

One anticipated benefit the centralized model didn't realize for AAO pertains to buy-in from organizational stakeholders. This finding, however, is perhaps not surprising given the security group's lack of authority. For instance, the centralized SMM was unsuccessful in getting policy implemented because management didn't see the benefits of the policy relative to the likely disruption to business, possibly because security was a secondary concern for stakeholders. Alternatively, the policies might have been poorly designed: given that the centralized team was divorced from day to day organizational operations, the policies might have failed to reflect operational requirements. We speculate, however, that with increased management buy-in, the policy process would have gotten further. In particular, if policy usability was the issue, then management buy-in could have resulted in the security team refining the policy appropriately rather than abandoning it (as occurred with AAO). The lack of buy-in across the organization subsequently influenced security management consistency, which was a second aspect that was in misalignment with CERT expectations under the centralized model. In particular, the security group's inability to enforce policy and other security processes negatively affected the degree to which stakeholders consistently carried out security tasks within the organization.

AAO's experience with the centralized model highlights that merely being informed of significant security vulnerabilities isn't enough for users and administrators to address them, for instance, through a sense of civic responsibility. This implication is important for other organizations in which a security team won't have direct authority over all departmental units. We propose that if organizations or security teams find that they don't fit a specific model well, they take additional guidance from SMMs developed to work with some of the unmet key organizational aspects. For example, an organization might not originally consider the coordinating SMM described in the CERT guidelines because it's designed for teams external to the organization for which they're managing security, but this model does assume the team lacks authority over these organizations. Guidelines and strategies for security teams using this model could be helpful in an organization with fairly autonomous units.

Decentralized Model in Practice: Benefits and Drawbacks

At some point, AAO's goal with respect to security management shifted to emphasize embedding security within the organization, allowing the security team to conduct operational security-related duties. The organization accompanied this shift with a move to a decentralized model. When we analyzed the organization's experience with this model, we found three mismatches with the expected CERT guideline outcomes. As with the centralized model, the security team's lack of authority negatively impacted buy-in and subsequently consistency, leading to a misalignment with the CERT handbook expectations. Two unexpected misalignments, however, were the team's ability to effectively communicate with each other and to conduct security wide procedures such as audits and assessments.

We'd expect that the poor support a decentralized SMM affords for communication between security team members would be exacerbated in a team lacking a central security manager. However, the three distributed members from AAO's former security office still function cohesively in many ways. This could be due largely to the team's prior history of working in a centralized group. One management participant reflected on this loosely connected group's ability to maintain a presence in the organization. During a discussion of the system-design review process, he mentioned that a check box on the application asked whether it had gone through the (now distributed) security group. This participant reflected, "So then do you need a separate security group that [...] on the organization chart it actually shows up 'security group'? Or maybe we've advanced beyond that?"

One factor that might have bolstered the decentralized model's success is the lack of turnover in the security team. No turnover occurred within security staff since before the move to a centralized approach. The fact that these distributed security members worked so well together is likely due to their shared experience and tacit knowledge. A lack of formalized responsibilities and reliance on tacit and transactive knowledge will become a concern if one or more of these members leave the organization. We believe that the current structure will cease to be as effective over time if such factors change.

Organizational Evolution

One implication of our findings is that an organization's evolution through various SMMs provides experiences that can mitigate some of a given SMM's weaknesses, as with the example of the cohesive security team. As another example, consider whether the security team should have operational duties. A trade-off exists between understanding security in the context of the technology within a subgroup and having conflicting priorities between the organization's overall security and the subgroup's operational needs. One participant, for example, appreciated the understanding of the network that developed from being operational within the unit. On the other hand, another participant, less appreciative of the same component because it interfered with security tasks, described a security project abandoned due to lack of focused time. This participant did agree that the organization needed more operational security, but believed that it was better to achieve this by developing templates and procedures that operational

Security Management Models

We distilled the security management models (SMMs) and model attributes from the CERT guidelines.[1] Table A compares the extent to which each SMM supports the attributes as described in the guidelines and experienced by the case study organization.

Common Security Management Models

- *None.* There is no formal team and no formal security responsibilities assigned.
- *Centralized.* The security staff is centrally located in an organization (reporting to a central manager); team members typically devote close to 100 percent of their time to security.
- *Decentralized.* The security staff is interspersed throughout the organization (reporting to a central manager); team members typically perform both security and other IT duties.
- *Hybrid.* Both centralized and decentralized security staff (reporting to a central manager); typically, the centralized members perform high-level analysis or provide recommendations and policies, whereas those decentralized perform lower-level operational security duties.

SMM Attributes

- *Consistency:* degree to which security-related tasks are consistently carried out in the various organizational units;
- *Responsiveness:* extent to which security incidents are resolved in a timely manner;
- *Expertise:* extent to which security staff have security related expertise, including both proactive and reactive techniques, operational security, and new security technologies;
- *Commitment:* extent to which security staff are able to dedicate themselves to security-related tasks;
- *Communication:* extent to which the SMM facilitates internal communication between security team members;
- *Promotion:* extent to which the SMM facilitates external communication between the security team and other stakeholders, including security-related information dissemination, policy generation, and awareness;
- *Buy-in:* extent to which the SMM facilitates buy-in from various organizational members, including security practitioners (for example, to perform non-security operational tasks) and other stakeholders (for instance, to adopt policies).

Reference

1. G. Killcrece et al., *Organizational Models for Computer Security Incident Response Teams (CSIRTS)*, tech. report CMU/SEI-2003-HB-001 ADA421684, Software Eng. Institute, Carnegie Mellon Univ., 2003; www.sei.cmu.edu/publications/documents/03.reports/03hb001.html.

Table A. Strengths and weakness of security management models.

	None	Centralized		Decentralized		Hybrid
	CERT	CERT	Study	CERT	Study	CERT
Consistency	Low	High	Low	Medium	Low	Medium
Responsiveness	Low	Medium	Medium	High	Medium	Medium
Expertise	Low	Medium	Medium	Medium	Medium	High
Commitment	Low	High	High	Medium	Medium	High
Communication	Low	High	High	Low	High	Medium
Promotion	Low	High	High	Medium	Medium	High
Buy-in	Low	Medium	Low	Medium	Low	Medium
Procedures	Low	High	High	Medium	High	High

staff could use without involving security personnel. This participant wanted to return to a central SMM with dedicated security staff. Furthermore, he felt that the central security office was technically diverse enough because its staff came from different IT backgrounds and had different system focuses; being embedded in the different subgroups wasn't necessary.

We can't determine the effectiveness of an organization's defense against Internet attacks only through its choice of firewalls, intrusion-detection systems, patching, and antivirus tools. The IT security professionals who select, deploy, administer, and troubleshoot that organization's defenses and respond to security incidents are supported and handicapped by the structure and dynamics of the corresponding processes. An SMM's fit for a specific organization also impacts the overall effectiveness of the organizations defenses.

Throughout our findings, a common thread has been the challenges that result when implementing an SMM that doesn't fit completely with an organization's underlying attributes. The shifts between the various models in AAO occurred due to both attempts to mitigate negative organizational influences, such as lack of authority, and shifting organizational goals. In particular, our organization chose a centralized model to support its goal of having a dedicated staff for promoting security culture and measures in the organization. Although the centralized model was effective for this aspect, a new competing goal emerged when some security team members needed to become more "operational" in their daily tasks, thereby providing the push for a decentralized model that afforded doing so.

On the one hand, we certainly agree with the CERT guidelines[4] that organizations need to educate themselves about various SMMs to benefit from established best practices. On the other hand, perhaps a meta lesson to take away from our findings is that SMMs need to evolve with an organization to adjust to its shifting priorities. In these shifts, as our case study illustrates, the team members' prior experiences impact the process, as they enter each SMM bringing with them new expertise and perspectives. Although the "pendulum swing" between various IT governance models has drawn criticism in the past,[8] AAO's experience gives a hope that, with each "swing" between SMMs, an organization might find itself able to incorporate more of its prior practices, in essence moving toward a hybrid model with attributes customized to and most appropriate for the organization.

References

1. D.A. Siegel, B. Reid, and S.M. Dray, "IT Security: Protecting Organizations in Spite of Themselves," *Interactions*, May/June 2006, pp. 20–27.
2. A. Brown and G.G. Grant, "Framing the Frameworks: A Review of IT Governance Research," *Comm. of the Assoc. for Information Systems*, vol. 15, 2005, pp. 696–712.
3. *Information Technology Security Techniques — Code of Practice for Information Security Management*, International Standards Organization, 2005; http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297.
4. G. Killcrece et al., *Organizational Models for Computer Security Incident Response Teams (CSIRTS)*, tech. report CMU/SEI-2003-HB-001 ADA421684, Software Eng. Institute, Carnegie Mellon Univ., 2003; www.sei.cmu.edu/publications/documents/03.reports/03hb001.html.
5. D. Botta et al., "Toward Understanding IT Security Professionals and Their Tools," *Proc. Symp. Universal Privacy and Security*, ACM Int'l Conf. Proc. Series, vol. 229, 2007, pp. 100–111.
6. K. Hawkey, K. Muldner, and K. Beznosov, *Searching for the Right Fit: A Case Study of IT Security Management Model Trade-Offs*, tech. report LERSSE-TR-2007-03, Laboratory for Education and Research in Secure Systems Eng., Univ. of British Columbia, 2007; http://lersse-dl.ece.ubc.ca/search.py?recid=139.
7. D.M. Wegner, "Transactive Memory: A Contemporary Analysis of the Group Mind," *Theories of Group Behavior*, B. Mullen and G.R. Goethals, eds., Springer-Verlag, 1986, pp. 185–208.
8. D. Lewis, "IT Governance: Stop the Pendulum!" *Computer World*, 12 Jan. 2004; www.computerworld.com/managementtopics/management/story/0,10801,88888,00.html.

Kirstie Hawkey is a post-doctoral research fellow in both the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) and in the Department of Computer Science at the University of British Columbia. Her research interests include usable privacy and security and personal information management, particularly within the context of group work and assistive technologies. Hawkey has a PhD in computer science from Dalhousie University. She is a member of the ACM. Contact her at hawkey@ece.ubc.ca.

Kasia Muldner is a post-doctoral research fellow at the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) at the University of British Columbia (UBC). Muldner has a PhD in computer science from UBC. Her research interests span human-computer interaction, including usable security, as well as artificial intelligence and cognitive science. She is a member of the Association for the Advancement of Artificial Intelligence (AAAI). Contact her at kmuldner@ece.ubc.ca.

Konstantin (Kosta) Beznosov is an assistant professor at the University of British Columbia's Department of Electrical and Computer Engineering. He is the founder and leader of the university's Laboratory for Education and Research in Secure Systems Engineering (LERSSE). Beznosov has a PhD in computer science from Florida International University. He coauthored Enterprise Security with EJB and CORBA (John Wiley & Sons, 2001) and Mastering Web Services Security (John Wiley & Sons, 2003) He is a member of the IEEE and the ACM. Contact him at beznosov@ece.ubc.ca.