Searching for the Right Fit: A Case Study of IT Security Management Model Tradeoffs

Kirstie Hawkey[*], Kasia Muldner[†], Konstantin Beznosov[‡]

Laboratory for Education and Research in Secure Systems Engineering

lersse.ece.ubc.ca

University of British Columbia

Vancouver, Canada

Technical report LERSSE-TR-2007-03[§]

Last Modification Date: 2007/11/16

Revision: #12

[*] hawkey@ece.ubc.ca

[†] kmuldner@ece.ubc.ca

[‡] beznosov@ece.ubc.ca

[§] This and other LERSSE publications can be found at lersse-dl.ece.ubc.ca

Abstract

The usability of security systems within an organization is impacted not only by tool interfaces but also by the security management model (SMM) of the IT security team. Finding the right SMM is critical and yet can be challenging, as there are tradeoffs inherent with each approach. We present a case study of one post-secondary educational institution that created a centralized security team, but disbanded it in favour of a more distributed approach three years later. The case study consists of interviews with ten IT staff from across the organization who gave us their diverse perspectives of the realities of managing security in a decentralized post-secondary organization. We contrast this organization's experiences with SMMS with expectations from industry standards and derive organizational factors that impact the success of the models. These factors highlight the importance of considering both the organization's security goals as well as its structure when evaluating potential SMMs. Furthermore, top management support, security policies, and a security team with vested authority, along with the organization's prior security management history, impact the success of a given SMM.

Contents

1 IT Security Management Models

Information Technology (IT) has moved from the sidelines to play a center stage role in today's organizations. This growth has brought with it a set of challenges, a key one of which pertains to security. Security incidents are costly to organizations; much work remains to be done before it is understood how to best support security practitioners in their daily tasks. The ability of an organization to protect itself from IT attacks is determined not only by the usability of the security systems within the organization, but also by organizational factors. One such factor is the security management model (SMM) adopted by the organization.

What constitutes a suitable SMM for security professionals in an organization is a hotly debated topic. The recent push for IT Governance as a result of legislation, such as the Sarbanes-Oxley Act, has highlighted the need for more formalized accountability structures. To date, however, the majority of research has focused on IT governance models, without specifically examining IT security management [1]. Since IT security distinguishes itself from general IT in a number of ways, this complicates the application of IT management guidelines. A notable exception is the generation of security standards by organizations such as ISO/IEC [2] and CERT [3]. In particular, a key tenet identified in these standards is that the security team includes a manager who is centrally located within the organization. What is less clear is where to position the remaining security team members within the organization. Consequently, an organization may swing from one SMM to another, after discovering the hard way that the SMM originally adopted was not the right fit.

Traditionally, the two basic SMMs include the centralized and decentralized structures. In a centralized model, a centrally-located team of dedicated staff devote all their time to upholding security. In a decentralized model, on the other hand, security is upheld by practitioners who are integrated into other teams. Each model has unique advantages and disadvantages, leaving some to argue that a hybrid model is the solution to security management. We illustrate the benefits and challenges of SMMs in practice with a case study of ten participants from one organization that established a central security management office and then disbanded it in favour of a decentralized approach.

From this case study, we derived several key factors that we believe should be considered when evaluating the tradeoffs of the security models to determine the best SMM fit for the organization. These factors can be summarized as the following lessons:

1. The tradeoffs between various SMMs need to be considered not only in light of the industry-standard proposed best-fit, but also in terms of an organization's priorities with respect to SMM attributes.

2. The characteristics of an organization's structure can heighten or lessen the importance of various attributes of an SMM.

3. Top management support of policy development and an investment of authority in the security group are necessary to increase buy-in across the organization.

4. An organization's evolution through various SMMs provides experiences that can mitigate some of the disadvantages of an SMM.

We first present a chronological case study of one organization's experiences with security management models. We then discuss the anticipated benefits and disadvantages of each model, using the CERT SMM guidelines for security incident response teams [3]. Finally, we present the lessons we derived as a result of comparing the experiences of our case study organization with the anticipated outcomes as a result of the SMM in place.

2 One Organization's Experience

The case study is part of the on-going HOT-Admin project, which aims to devise effective solutions for supporting security practitioners in protecting organizations from IT-related attacks (see [4] for preliminary results). In contrast to traditional approaches that focus on technological aspects of security by evaluating the usability of security tools in controlled laboratory settings (e.g., [3]), we argue that devising effective solutions requires investigating all the factors that impact security practitioners: the human, organizational and technological (HOT). Therefore, as a first step in attaining the HOT-Admin goal, the focus has been on gaining an understanding of the impact of these factors on IT security through a field study. Specifically, we have been conducting in situ semi-structured interviews with 26 IT professionals, all of whom play a role in upholding security in their organizations. The participants belong to a wide range of organizations (11 in total: three post-secondary educational, two scientific services, two consulting, one manufacturing, one insurance, and one non-profit organization).

Here, we focus on a case study comprising ten of the interviews from one of the post-secondary educational organizations. This institution is a large distributed organization that includes in its central core a IT Services unit, referred to as Central IT (see Figure 1) and over two dozen external distributed departmental units. Central IT provides IT-related support to the organization, including: (1) infrastructure, e.g., network and wireless management, (2) delivery of core applications, e.g., e-mail, (3) strategy, e.g., maintain relationships with the organization's stakeholders, (4) IT support, including outreach and identification of IT services that need to be supported, and (5) finances for the Central IT unit. Central IT is also responsible for overseeing the organization's IT security. This case study will describe the progression in security management models from no formal model, to a separate security office, to its dissolution three years later to a decentralized model with its former members integrated into the various units within Central IT.

The participants in our case study work in a variety of departments across the organization. As Figure 1 illustrates, five participants were from the various units within the organization's Central IT department, and corresponded to two IT security staff, a director whose title at the time of the interview was security manager, an IT director, and an IT administrator who performed some security duties. The other five participants belonged to two separate faculties, labeled A and B in Figure 1, within the decentralized organization. Faculty B was a large and diverse microcosm of the organization itself, that included a central IT core that housed three of our case study participants. Two of these participants held the position of IT Manager, while the third was IT security staff. Finally, the remaining two participants, worked as IT administrators for small departmental units within Faculties A and B, respectively. To preserve the anonymity of our case study participants, we avoid participant numbers and other identifiers in the subsequent text.

Our case study organization faces a number of security-related challenges. One challenge stems from the academic nature of this organization, specifically its openness. This not only makes policy enforcement difficult, but also means that accessibility and sharing of information is encouraged. Security practitioners are left with the difficult task of protecting private and confidential information, IT labs, and individual machines. A second security challenge mentioned by our participants was the organization's diversity and its decentralized structure, a characteristic shared by many of today's organizations. These units are varied with respect to size, the degree of resources to devote to IT security, and the set of activities that need to be supported. This diversity complicates the generation of consistent policies; furthermore, communication across the distributed organizational units can be

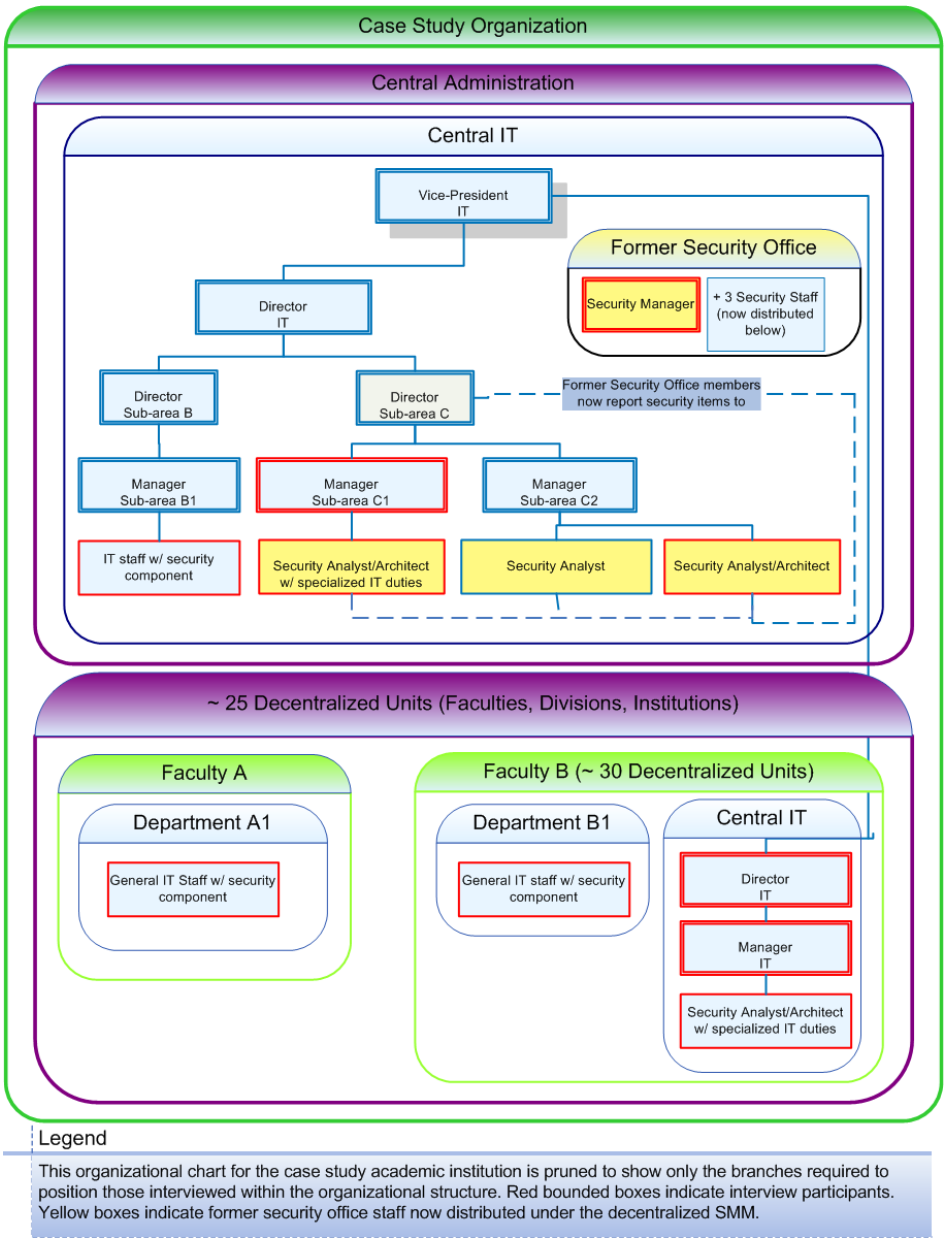

Figure 1: Structure, distribution of participants across the organization, and classification of participants' positions in the studied organization

difficult.

Given the security related challenges, the organization has undergone several reshuffles with respect to its security team. We now describe its experiences as it transitioned between IT security management models.

2.1 Emergence of a Centralized Security Team

Until a few years ago, the organization had no formal IT security team, although several of the IT staff within the Central IT department were security minded. For example, one of our participants stated they were one of the first of the IT staff to be interested in security. This participant gradually performed more security responsibilities and over time began to specialize in security. While this participant took a few formal security courses, much of their security knowledge was self-taught through attending security conferences and reading security magazines and on-line publications.

Before the formation of the central security office, representatives from different groups within Central IT formed a very loose security team. They met on an informal basis and talked about a variety of security issues and projects. Some of the managers also attended these meetings from time to time and would attempt to find funding and resources to implement security-related projects. The issues and projects discussed by this loose team appear to have been limited to Central IT as the security-oriented individuals within Central IT reportedly charged out their time to other departments with security needs.

The security office was formed in 2003 and consisted of a security manager hired into that role and three dedicated security professionals. Two of the team members were technically inclined and one had extensive experience administering the organization's responsible use policy. The formation of the central security office was part of a move by the Central IT department towards a more cooperative management model. A shift towards cooperation was a deliberate focus of the central security team and the security manager was hired into the role because of their cooperative approach. Cooperation and communication were deemed to be necessary in such a large, decentralized organization. The security office served the greater organization as well as the Central IT department: "The security office within Central IT has a dual role. It acts both as the security group for the internal IT department and that's where it has project oversight and that sort of thing, but it also has a broader mandate to

ensure the security of the entire [organization]. Now because it's a very decentralized organization, the central security group doesn't have a lot of direct authority or control over the end users in the departments and so with the departments, it's a very open communication effort saying: here are best practices, here are the things we are doing at the central level, here are resources for you when you're doing security for your department."

This focus on communication and cooperation was reflected in the measures of success for the performance reviews of security professionals within the central office. These included their skill at communicating with end users (both within Central IT and across the organization), how well they contributed to the public discourse about security within the organization, as well as how proactive they were at dealing with security threats.

A key aspect of the organization's IT governance strategy was to embed security into both the project process and the change management process. The security group conducted formal reviews and signed off on projects at both the design and implementation phase. During the design phase, they reviewed plans and made sure that security was taken into consideration. On large projects, they worked in conjunction 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 had to go before a weekly meeting of the change approval board. The security team played a key role in these meetings and held veto power over changes that would compromise security. Unless an emergency, changes were scheduled and time allotted for the testing and review process.

In addition to security assessments, the responsibilities of the security office included security oversight for the organization, the development of security policies, and security enforcement. The central security office used a split security model of awareness and enforcement. The security manager played the security awareness and advice function within the organization, while the enforcement function was largely handled by the internal audit department. While the security team members were not necessarily responsible for operational security, during the existence of the central security office, their main activities included the implementation of VPNs and firewalls. However, although the team originally had the goal of developing a centralized monitoring system, this goal was not realized.

Several benefits were anticipated by members of the security team as a result of the creation of the central security office. The team members were pleased to be following the trend towards centraliza-

tion of security. With a manager and a budget for security, they did not have to fight for resources. They also did not have to convince other people (at least within their group) of the importance of security. Indeed, security was recognized to be a rapidly evolving, and the security office members were supported with a training budget higher than the standard 5% within Central IT. However, there was also some anticipation of challenges associated with being a new group within Central IT, trying to balance the potential of new IT security projects with a lack of experience across the organization. We next describe participants' experiences with the central SMM. Where appropriate, we reflect on the impact of the model on their security-related activities.

2.2 Experience with the Centralized Security Management Model

Under the centralized security management model, triage of security incidents was a responsibility of the security office. Notification of incidents occurred through phone calls, emails, and tool alerts. One advantage of centralization was that the security professionals were able to take a proactive approach to security incidents, maintaining an overview of security vulnerabilities for the organization. Not having operational tasks allowed them the time to learn about new vulnerabilities, to develop scripting tools to check for signs of exploits, to scan systems in both Central IT and the overall organization for problems, and to assess any problems found. However, the security office did not generally fix systems affected by the incident, but would forward the information to the correct departmental IT staff.

To improve collegial relationships and encourage security awareness across the organization, the central security group made an effort to be accessible. They saw communication as integral to the job of being a security person in the organization and, as such, were open to receiving phone calls and emails, and did not treat communication attempts as intrusions that took them away from their work. This level of availability was not felt to be disruptive as they did not have a large amount of operational responsibility. Indeed, this lack of operational responsibility was viewed as strengthening security within the organization: "I think that if you are an operational folk, it is the phone calls and the e-mails that kill you, and that distract you from your job. One of the reasons security gets compromised, are the interruptions [of operational folks]. [Having a security group] focused on outreach awareness, best practices, oversight, rather than day to day operations has been a great asset in being able to respond in a friendly manner to those requests."

Our interviews captured many stories of communication between security team members and those from other departments both within Central IT and across the organization. Communications varied from informal conversations in the hallway, to face-to-face meetings to tease out security issues and requirements, to more formal requests for assistance initiated through contact from a group manager to the security manager. The strongest benefit of the central security office in terms of communication may have been a well-established single point of contact: "The security group is also in the position to be that one stop point of contact around security issues for the campus. If you have a security question, if you need advice, on security architecture or administration [our] security group has always been open where anyone on campus can come".

There were, however, some challenges associated with a lack of authority in the decentralized organization. While the dedicated security staff had an improved ability to collaborate and coordinate with departments across the organization, they did not have the ability to mandate security measures within the departments. Their efforts at communication were seen as a way to mitigate this lack of authority: "in other organizations where security has more tools, more teeth, more power in some senses, they don't necessarily have to be as open and communicative".

The central security office was in existence for approximately three years. It was viewed as successful in the opinion of at least half of its team members. Indeed, the success of some of its initiatives is evidenced in procedures that are still in place today. For example, the security review during system design phases and the procedures for security incident response have not changed since the group's dissolution. However, as discussed next, the central security group was not as successful at creating policy. One participant recounted how the policy did not have the reception they expected from the organization and the project was dropped. This participant thought that the policies were not viewed to be as "sexy" a concept as the firewalls that were being installed everywhere.

The lack of management support for policy development may have been due to the management not viewing the benefits of the policy as clearly as the disruption to operations that might arise as a result of the policy. Security is often viewed as a secondary concern to business operations [4]. Formal policy change is difficult and time consuming, particularly for a decentralized academic organization. For example, the responsible use policy that came into effect several years ago was reviewed by all the stakeholders, including lawyers, students, faculty, staff, and every organization on campus. Policies must be flexible enough to apply to many institutions and it is common to re-draft the procedures

section of a policy to suite new circumstances/interpretations rather than go through the formal policy change process. The central security office may also have been too divorced from the day to day operations to realize the full implications of their suggested policies on IT practices.

2.3 Dissolution of the Central Security Office

There are a number of events that coincided and led to the dissolution of a formal central security office about one year ago. With the creation of the central security office, the security management model had shifted in recognition of the decentralized nature of the organization, attempting to raise awareness of security throughout the organization: "decentralization can work if there is a lot of communication, if there are central resources that can be drawn on where needed [...] so that's certainly how we've tried to mold the security organization, by being frequent speakers at departmental meetings [...] at those kinds of things". However, with the centralized SMM, there was a perception that security was too divorced from operations. One of the three security professionals within the office was actively lobbying for a more operational role. This employee was frustrated not to be involved in the implementation of IT security controls. The lack of an operational role meant that the security office was limited to giving security recommendations, relying on other specialists within the IT organization to reconfigure affected devices. However, the other groups, which already had enough work with their own activities, were often resistant in taking on security-related tasks. This participant was unsure of all the factors behind the decision to dissolve the security office, but had the perception that it may have stayed if the security group had the authority to impose recommendations. For this participant, a move to a decentralized security management model which allowed the security specialists to implement needed security measures was necessary given the lack of authority across the decentralized organization.

This perception that security should be embedded within the organization because it is an integral component throughout the organization was echoed by another participant: "Security doesn't stand on its own because it's not just the network, it's also systems, it's also the host, and it's the applications as well. So you need to have security involved in all of those. So you need those aspects in all of those other areas. Because we have organized Central IT more along kind of functional boundaries, then you need to have that security function across all of them. [...] if you segmented it up that way [along services] you still have to have security kind of aware in all of those as well. So it doesn't matter which

way you do your organization, you still have that kind of band of security going through."

It is also questionable how much top management support there was for the central security office. As discussed above, there appeared to be limited support with respect to development of security policies and the implementation of centralized monitoring of security incidents. However, it does appear that management support for policy development may be increasing. In an interview conducted shortly after the dissolution of the security team, one participant noted that "there is a current lack of formal policies that vest a lot of authority in any group to deal with security"; however, this participant went on to say that they were developing an overarching security policy "that doesn't necessarily say exactly what you need to do to secure your systems, but does vest the authority for coming up with procedures and best practices and giving enforcement powers to a central security group". These comments suggest that there is some top management appreciation for a central security group with the authority to deal with security issues. However, another participant, interviewed a few months later, stated that the group has not been very successful recently getting security projects approved because of other operational priorities. This participant felt that a lack of recent security incidents was a factor in the reduced resources available for security projects: "there is probably enough security happening at this point that it is not at the very top of the list that we must do this". Another echoed this perspective: "I think security is just one of those things that get kind of, well, there's nothing happened and it would just be shoveled aside and oh, keep on with all the operations, all the projects that are on hand. We serve the customers and then all this security is put at the side".

2.4 A Shift to a Decentralized SMM

Despite the perception of management support for investing authority in a centralized security group, when the security manager received a promotion about one year ago, the position was not filled. There is still some support within Central IT management, however, for a central security manager: "We don't have a security manager at this point. We did at one point, but we have done a little bit of reorganization, so we don't actually have one right now. We have been discussing about do we need a security manager or not, and we haven't made any decision yet that way or not. I think personally we should have one because it's easier to have that one person to be able to point to and say okay, we have a security issue you have to take care of it; use the resources that you need to, even though they are across the organization."

Several months later, the central security manager position has yet to be filled. In fact, the security office remains as a facade only; however, its presence can be found on a web page and in student handbooks. The other three security practitioners can now be found distributed within two of the Central IT departments. They are still the only three within Central IT with security as their main focus: "There is probably three people who spend the majority of their day having to do with security issues and one of them is in [the networking area], so that's kind of the software parts of networking. One is in the systems group, and so is dealing with like system-type post type security type issues and the other person is also in the systems group but is taking care of more of the responsible use kinds of things". Their responsibilities under this decentralized SMM include security related tasks such as policy development, review of new system design, participation in the change management process, responding to emails and alerts of potential problems, checking logs to look for possible intrusions, and responding to threats and incidents, as well as more operational tasks such as taking care of network security appliances, centralized management of many of the firewalls, and standard network administration.

The three distributed members of the former security office still in many ways function as a cohesive group, despite their lack of a formalized structure. One described their current situation as: "Not ad hoc, we do it kind of regularly, but there's nothing really formalized in terms of okay, we have this committee, and we have a list of tasks [...] this is just how it is working now — it's just like a transition we have, it's not really worked out yet, about division of tasks, in setting priorities." As an example of cohesion, the general contact email address (security@[organization]) and phone number for the former security office are still active; email triage is still handled by the members of the former security office. The responsible use coordinator is the main point of contact, but the other two also monitor the emails. They rely on transactive memory to judge who will pick up certain items on this email list as well as on email lists specific to other groups that they monitor: "people are going to assume if there's a firewall component or a security component or if there's something that they know I'm going to be responsible for, they'll just assume that I'm going to get it, so you have to sort of read everything".

One of the former members has been informally placed in the role of coordinator by senior management and has been tasked to expand the group into a committee, including representatives from other teams, so that they can have meetings and talk about the issues. The former members are currently meeting 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, problems, just whatever". However, the expansion to a broader committee that includes others from across the organization has not yet been realized: "But it is just that up to this point we have people engaged in policy and each of us has our own work to do within our respective teams, so we just don't have time for yet another kind of committee, we just don't have the time to do it. So we may as well not have it now until there is a need to do it".

The reporting structure is also in transition and quite informal. Currently, one of the directors has "taken on a bit of that role of managing information security — not at a real in-depth level, but just for if there are any particular policy issues and things like that that come up at this point. So they meet with [director], but it's not really a reporting structure. It's a meeting of 'okay what are the actions that we are working on' and [director] is kind of directing what are the main things that need to be done. It's kind of an odd situation, but that's what we're working on at the moment". One of the managers of a distributed team member also discussed getting reports on behalf of the team through the employee embedded in the group. "Just for being able to track what it is they are working on. Just to know kind of in general what kinds of things there are, like about how many kinds of complaints we are getting, that kind of thing".

2.5 Experience with the Current Transitional Model

Policies were perceived to be necessary to promote awareness of security procedures and the importance of security: "I think all organizations should have policies so that all staff is aware of what is expected of them, their responsibilities, and the importance of security in general". Furthermore, this participant went on to describe that it was also important that detailed procedures and guidelines be provided to help staff achieve compliance. One of the managers discussed the current state of policy development within the Central IT department: "We don't actually have any set security policies in place at Central IT. Like what is the security policy for your laptop or for your host station? [...] Must everyone use the VPN service? You know - those kinds of things. They are in draft form but they haven't actually gone through the rest of the steps, through the management to say okay these are policies that everyone has to abide by. So they've actually been working the last while on getting the drafts in a more final kind of state and then those should get approved I hope quite soon actually. And then there is an implementation process to go through".

Security incident response appears to be handled in the same fashion as when under the centralized security management structure and one participant stated that they did not think that the decentralized SMM impacted 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 or not something 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 of the current transitional model is that without a security manager and an enforceable security policy, the informal group must sometimes escalate their security incident responses to somebody with the ability to enforce their request for action: "By and large the group functions quite fine normally on a day to day type of basis, like if there are complaints that come in and they take care of them, whatever type of complaint it is. You know, somebody may be causing an attack or is being attacked, it's kind of one or the other type of thing. There are procedures in place for dealing with those and if they run into problems with those, and it can be all kinds of things — where the person causing the attack or being attacked isn't being very cooperative, then they will need a manager to get involved or the director to get involved in it if it's a particularly difficult situation to deal with. But they escalate those. "

Policy creation appears to be going well under this current model, although the success is likely less due to the model than because of the external forces driving policy development. The organization currently must draft and implement internal security policies and procedures for servers and workstations in order to achieve Payment Card Industry (PCI) compliance, so policy development has become a high priority for the organization. The policy committee is led by one of the former security office staff and was to include managers and other representatives from the affected groups as well as the rest of the distributed security team; however, the managers have not been attending meetings. This lack of managerial participation is making it difficult for the committee to iterate on the drafts; the IT and security staff present in the meetings can describe usual practice, risks, and procedures to mitigate the risks, but it is up to the managers and senior managers to actually set the policy and approve the budget for providing the necessary infrastructure for policy implementation.

One of the intended benefits of distribution of the security members into Central IT's subgroups was an increased awareness for security within those groups. This awareness appears to be realized, at least for those two groups who received the distributed staff: "It's been really helpful to move people from being in just a specific security group, because they were kind of separated then, to move

them into pieces of the organization. Because then it's more of an awareness of security that happens throughout the organization. And I think that that has been beneficial". Moreover, the distribution helps the security people be aware of what is going on within the subgroups of Central IT: "It's like — you know like sometimes they got involved in things and sometimes you forgot to tell them about something or they don't know about an incident that's going on". This participant described how including the whole group on emails about security incidents and trouble ticketing fosters the development of tacit knowledge and provides awareness of incidents to which they may be unknowingly contributing.

However, one area where awareness may be reduced is the central overview of security for the organization as a whole, which was a benefit of the centralized model. Under the current decentralized SMM, with the practitioners also having operational tasks within their individual departments, there is less of a focus on overseeing the whole campus as well as less time available to do so. At least one security practitioner is still trying to maintain an overview: "I need to have a feel of the activities on campus. It gives me an idea of if, say, a lot of computers on campus are compromised or whether it's very quiet and there's nothing happening much". This participant also expressed some frustration at the lack of cooperation across the organization in developing this overview through confirmation of whether or not current exploits are the underlying cause of an incident: "until we actually get results from the network administrators to report back as to what they find, we don't know. Some administrators, not all of them, do a thorough job, because they are not, how should I say that, they are not obliged? There is no obligation on their side to report back". This same participant expressed a concern about having insufficient time to keep abreast of the latest vulnerabilities.

It is this operational aspect of the distribution that appears to heavily affect perceptions of the transitional management model's success. There is a tradeoff between the benefit of understanding security in the context of the technology within a sub group with the downside of having conflicting priorities between the overview of security for the organization and the operational needs of the sub group. For example, one participant was very appreciative of the operational aspect as it allowed him to "understand the network in a sort of 360 degree way. So the only way to fully understand what's happening in your network it to support it I think and participate in its design". On the other hand, another participant was less appreciative of the operational component because it was interfering with security tasks. For example, this participant described a security project that was abandoned due to lack of time: "so at one time, I just have to give up because I have so many other things to work on. In this

task you need to concentrate your effort on it for a length of time without other interruptions". This participant does, however, agree that there is a need for more operational security, but believes that it is better done through developing templates and procedures for operational staff to use, rather than having a security person do it: "other people, at this point they kind of rely on us to do what needs to be done. But we are trying to have more people be security conscious. It's getting better, a lot better than before, but it is still — if everybody can work in IT and have this awareness, it would be a better place, I would say". This participant expressed a preference to return to the central security management model again: "It would be god to have an ISO, I mean a kind of a formal set up, with the people dedicated just to security, like before". This participant felt that the central security office was technically diverse enough as a result of its staff coming from different IT backgrounds and having different system focuses that being imbedded in the different subgroups was not necessary.

Although it is unclear if it is attributable to the security management model, security training has been increasing across Central IT, both within the two departments with security members and also within other departments. For example, one of the former security office members and their new manager described in detail how most fellow IT workers were being trained to cover various security aspects of their position so that security was also distributed within this group as well as across the organization. This was felt to be of benefit for vacation relief, but also for increased tacit knowledge throughout the department so that they can as a group be more capable of giving security advice across the decentralized organization. Another participant from sub-group B1 (one of the Central IT groups without an embedded security person) described having an internal checklist of security issues to target and known vulnerabilities to try to avoid during system development and the extensive testing done of completed systems before deployment. This participant also recounted how two colleagues recently came back from a four day security course and gave a report to the rest of the team on what they had learnt.

It is also unclear as to the impact of the current security management model on communication. One participant thought that there was less overhead in communications within the department as obstacles to implement security controls have been removed: this participant does not have to give recommendations or ask another specialist to perform security configurations, but can do it personally. However, there may be more difficulties with communication without a central security manager to serve as the single point of contact.

3 Comparing the Experiences with Expectations

As we highlighted above in our case study of our organization's experience with SMMs, our participants felt that the various SMMs models had unique advantages and disadvantages. To see the extent to which the advantages and disadvantages as outlined by industry standards matched our participants' experiences, we compared the two. The Sidebar summarizes the advantages and disadvantages of a set of security management models along a number of dimensions, as proposed by the CERT standard (see sidebar for a summary of the different SMMs). We found that our participants' experiences match the standard's expectations in SMM experiences along several dimensions (e.g., see *Expertise*, *Commitment* and *Promotion* for both the Centralized and Decentralized models). However, this was not always the case (e.g., see *Consistency* for both the Centralized and Decentralized models; *Responsiveness* for the Decentralized model). We suggest that a possible reason for this mismatch between standards' expectations and actual experience is due to a number of factors that must be considered when evaluating the tradeoffs of models.

1. *Consider organizational goals when evaluating SMM tradeoffs.*

   A key goal of our case study organization was to promote security across the organization. Doing so effectively was particularly critical given the academic nature of our organization: such organizations typically do not have complete authority to enforce policies, and so must rely on other means, such as ensuring that their units are security conscious. To achieve this goal, the organization chose a centralized model that has the advantage of a *dedicated* security team, i.e., since the security team members are only responsible for security tasks, they have the resources to carry out proactive measures, such as promotion of security.

2. *Organizational structure can heighten strengths and weaknesses of a given SMM.*

   The CERT guidelines suggest that a centralized SMM may not the best fit for a large decentralized organization with diverse units; however, they also suggest this model may be appropriate for a large educational organization if the decentralized units have common characteristics. Although the latter was the case for our organization making the centralized SMM in theory a good fit, some of the disadvantages of a centralized model were exacerbated in our organization. We believe this was largely due to the organization's decentralized nature. In particular, with the centralized SMM, there was a perception that security was too divorced from day to

SIDEBAR

The security management models (SMMs) and attributes of the models were distilled from the CERT guidelines [3]. Table A provides a comparison of 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 100% of time to security.
- **Decentralized:** The security staff is interspersed throughout 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/provide recommendations and policies, while those decentralized perform lower-level operational security duties.

SMM Attributes:

- *Consistency*: degree to which security-related tasks are consistently carried out in the in the various organizational units
- *Responsiveness*: extent to which security incidents are resolved in a timely manner.
- *Expertise*: extent to which the 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 communication between security team members.
- *Promotion*: extent to which the SMM facilitates communication between security team and other stakeholders , including security-related information dissemination, policy generation, and awareness.
- *Buy-in* extent to which SMM facilitates buy-in from various organizational members, including SPs (e.g., to perform non-security operational tasks) and other stakeholders (e.g., to adopt policies).
- *Procedures*: ease that organization-wide procedures such as security audits, reviews, assessments, and change management processes can be conducted.

	SMM					
	None	**Centralized**		**Decentralized**		**Hybrid**
	CERT	CERT	Study	CERT	Study	CERT
Consistency	*	***	*	**	*	**
Responsiveness	*	**	**	***	**	**
Expertise	*	**	**	**	**	***
Commitment	*	***	***	**	**	***
Communication	*	***	***	*	***	**
Promotion	*	***	***	**	**	***
Buy-in	*	**	*	**	*	**
Procedures	*	***	***	**	***	***

Legend: *: low, **: medium, ***: high

day operations, possibly because the centralized office was too isolated from the distributed units.

3. *Top management support, policies, and authority impact an SMM's success.*

   Throughout the interviews, a common thread was the lack of *buy-in* across the organization and the lack of authority of the security group. The combination appeared to decrease the effectiveness of both security management models used. For example, one area in which the case study organization did not achieve the expected benefits of a centralized SMM was with respect to *consistency* in the application of security measures across the organization. In order to have success with the centralized SMM (and indeed with all models), there is a need for policies to communicate the security standards of the organization and for the security team to have the authority to implement and enforce those policies.

4. *The organization's prior experiences impact success of the SMM.*

   An organization's evolution through various SMMs provides experiences that can mitigate some of the disadvantages of an SMM. For instance, contrary to expectations as outlined by CERT standards, we found that the security professionals in our organization were able to effectively communicate effectively under both the centralized and decentralized SMMs. This is not expected to be the case under a decentralized model. In our case study it is likely the result of the security team members having a long history of working together and of them being willing to invest the additional effort to meet in an ad hoc fashion. This highlights the fact that even under a decentralized SMM, there is potential for supporting communication between the security team members.

4 Conclusions

We have presented a case study describing one organization's experience with various SMM's. The current SMM is working fairly well for this organization; however, the future is uncertain. As discussed above, there may still be a plan to replace the security manager as part of the organizations IT governance plan. The three distributed security professionals are also supposed to be augmented by other security focused staff from Central IT departments to form a more inclusive distributed security

committee. One management participant reflected on the current ability of this loosely connected distributed group of security professionals to maintain a presence in the university community. During a discussion of the system design review process, one participant mentioned that there was a check box on the application for whether it had gone through the security group (this loose group of people). This participant then reflected, "So then do you need a separate security group that you know that on the organization chart it actually shows up 'security group'. Or maybe we've advanced beyond that, that we actually don't need that.

Although our participants' experiences in some cases matched industry standard expectations in terms of how a particular SMM's advantages and disadvantages, we found this to not always be the case. We suggest that a likely explanation is due to a number of factors impacting the fit of a given SMM. These factors highlighted the importance of considering both the organization's security goals as well as its structure when evaluating potential SMMs as both will impact the relative importance of attributes of a model. Furthermore, if there is a lack of top management support of security policies and a security team without vested authority, the success of given model will be decreased. Finally, the organization's prior security management history will affect its experiences when a new model is applied.

Interestingly, the search for the right fit in terms of a SMM in our organization is currently mirrored by one of its organizational units, specifically the central IT unit of Faculty B, a large, diverse faculty. As was originally the case with the organization's central IT unit, this faculty's central IT group recently underwent a SMM reshuffle, from not having a formal security team in place to implementing a centralized SMM, however, the security practitioners in this case also perform non-security tasks. This may change in the future, since the staff has expressed a strong preference for setting up a dedicated security only team. If these wishes are realized, then the Faculty will be exactly one full step behind the organization's Central IT unit in its security management practices. In both cases, it appears that the perceived benefits of a centralized SMM, and in particular its support for dedicated security practitioners, overshadowed their perceptions of its drawbacks for large decentralized organizations. It remains to be seen whether the centralized SMM will be a more suitable fit for this faculty which is itself inherently decentralized.

References

[1] A. Brown and G. G. Grant, "Framing the frameworks: A review of it governance research," *Communications of the Assocation for Information Systems*, vol. 15, pp. 696–712, 2005.

[2] "17799:2005," 2005.

[3] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "Incident management," https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/incident/223.html, 2005.

[4] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Towards understanding IT security professionals and their tools," submitted to the poster session at the USENIX Security Symposium, August 2007.