

IT Security: Protecting Organizations In Spite of Themselves

David A. Siegel, PhD | Dray & Associates, Inc. | david.siegel@acm.org

Bill Reid, CISSP | Microsoft Corporation | bill.reid@microsoft.com

Susan M. Dray, PhD, CHFP | Dray & Associates, Inc. | dray@acm.org

SPECIAL
SECTION
HCI &
SECURITY

IT SECURITY AS AN ORGANIZATIONAL FUNCTION

It is a mantra of our profession that any search for strictly technical solutions that do not take the human and organizational elements into account is doomed to failure. This becomes especially interesting when it is borne out in an inherently technical realm, populated with “techies.” In this article, we share highlights from a field study of IT security at three companies. In the winter and spring of 2005, we spent four hours interviewing and doing contextual inquiry with each of 30 IT professionals at three companies. All of these participants, who ranged from frontline IT professionals to the top level of IT management, had some role in IT security. For some, security was a main focus while for others it was a peripheral aspect of their responsibilities. The companies included:

- an extremely large and diversified company with over 100,000 employees worldwide and a highly decentralized structure
- a rapidly growing service company with approximately 40 locations around the US and about 8,000 employees
- a health care organization with about 3,000 employees

Our observations drove home the lesson that human and organizational issues are major factors in determining how comprehensively and successfully a company manages security issues. We saw much evidence that people at all levels in IT were struggling with “people

processes” and were more frustrated by them than by technical problems. Unfortunately, IT people often seemed ill-equipped and ill-positioned to deal with the people issues and with their organizational complications.

This emphasis on organizational issues does not mean that IT people involved in security were completely up to speed on technical issues, or that they followed ideal security practices themselves. Indeed, some of the “people and organizational issues” played out within IT itself, as well as within the enterprise beyond IT. Here are a few examples from our study:

- chronic water leaks in a data center that were not receiving high priority for repair
- a departmental security coordinator testing a new application on his own machine, which was not a test machine isolated from the network
- an IT professional with no anti-virus software on a machine he used to connect to the network remotely
- a misunderstanding of what was needed to meet governmental requirements regarding data privacy and security
- failure to require strong passwords, and situations in which passwords were widely shared, such as everyone in a part of IT having the same password
- infrequent patching and auditing of patch status on machines, and over-reliance on manual processes to



accomplish this (having to walk around to physically check machines)

- a broad tendency to downplay internal risks

Observations like these challenge the naïve image of IT security as a finely tuned corporate immune system, tripped up only by flaws in its technical defenses. Certainly software plays a role in creating vulnerabilities and the usability of software tools for managing aspects of security is far from perfect. However, security depends on the interaction of what the software makes possible, what human beings do with it, and how organizations address their vulnerabilities. Furthermore, software will be better designed if it is informed by an understanding of the organizational context of its use. It is the organizational and behavioral layer that we focus on here.

All of the companies we visited were having problems in the following areas, all of which are crucial to developing and implementing an effective IT security strategy:

- maintaining a holistic, comprehensive perspective on the issue; *current knowledge about the company's assets, their vulnerabilities, and the specific array of risks the company faces; organizational entities empow-*

ered to set policy, strategy, and priorities for the array of risks; decision-making practices that take tradeoffs into account systematically

- disseminating and institutionalizing practice through the organization; *methods for translating policy into specific practices; effective delegation and coordination; methods for documenting policy and practice so that they can be communicated and applied consistently, without having to "reinvent the wheel"; methods for monitoring and maintaining effectiveness of security efforts, enforcement, auditing, etc.*
- achieving an effective level of partnership with the larger business around security; *the ability to make security enough of a priority to gain necessary resources for security overall, and for specific initiatives; effective collaboration with business decision makers across the company, so that, for example, IT security implications of business initiatives can be addressed in the planning stages*

In the rest of the article, we describe a small sample of our findings that show how challenging these organizational requirements are and how they impact security.

OBSTACLES TO A HOLISTIC, COMPREHENSIVE PERSPECTIVE

Companies face many challenges in attempting to manage security holistically. In this section, we focus on two of the most critical ones we saw.

Integration Versus Fragmentation.

Not only did IT leadership in these companies often seem to lack a holistic concept of security, but separate security-related activities, such as back-up, patching, anti-virus, and firewall management, were not closely united under the same organizational umbrella. At a higher level, physical security, network security, application security, data security, privacy, etc. were typically located in widely separate work groups. In two of the three companies, the only place in the hierarchy in which all these different specialized branches of the IT security picture came together was in the person of the IT director or vice president, for whose attention security had to compete with a tremendous number of other priorities. In fact, some of these areas overlap with departments outside of IT, making integration and coordination even more difficult.

Another factor that contributed to the fragmentation of security was that people who had a significant formal professional commitment to IT security were very rare. For many IT people, responsi-





bility for aspects of security was embedded in their roles, both explicitly and implicitly, but for most of them security was a minor focus. These people differed widely in their technical backgrounds and security awareness, and their personal investment in security sometimes did not seem commensurate with the potential impact of their activities on security.

The fact that these organizations seemed to lack a way of addressing security holistically made it difficult or impossible for security to be managed in a consolidated way, with consideration of the tradeoffs and prioritization among different security activities and initiatives. Indeed, none of these companies seemed to engage in this kind of systematic tradeoff analysis. Even a company that did have a high-level committee charged with guiding the company's approach to security had difficulty with this kind of systematic analysis. Across the board, security initiatives tended to be made of isolated tactics, not tied together by any overall strategy.

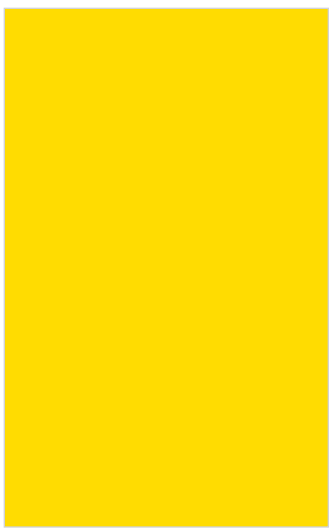
Blinders About Key Risks. In order for risks to be systematically evaluated and weighed against each other, they have to be recognized. In addition to what looked like laxness about certain areas of risk, there also seemed to be recurrent "blind spots." Particularly interesting was an apparent bias toward discounting risks of internal malicious or inappropriate behavior. The only internal users who caused concern were consultants or temporary staff who had access to systems. We heard a number of rea-


sons for downplaying internal risks:

- Everything is logged.
- We know each other.
- Everyone has signed nondisclosure agreements and statements of company policy about security.
- A couple of people who accessed "off-limits" data were fired, which serves as a warning to others.
- There is more risk from user errors and accidents than from maliciousness.

Was this kind of thinking a sign that tradeoffs were being weighed and that the de-emphasis of internal risk was justified? Not likely. Much data indicates that internal factors ranging from carelessness to malfeasance are the biggest sources of risk, and the fact that some damage is unintentional does not mean the risk should be discounted. For example, a recent article (www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey) reported the following statistics from a survey by McAfee:

- One in five workers (21 percent) let family and friends use company laptops and PCs to access the Internet.
- More than half (51 percent) connect their own devices or gadgets to their work PC.
- A quarter of these do so every day.
- Around 60 percent admit to storing personal content on their work PC.
- One in ten confessed to downloading content at work they shouldn't.
- More than half (51 percent) had no





idea how to update the anti-virus protection on their company PC.

- Five percent say they have accessed areas of their IT system they shouldn't have.

Behavior such as this represents serious security risks, because it can expose company assets to malware and confidential data to prying eyes.

As we began noticing this pattern, we started posing some hypothetical situations to test the limits of the rationales. For example, we asked, "Would any steps be taken to increase monitoring during a period in which there was an increased likelihood of a person being a "disgruntled employee," such as after a negative performance evaluation?" In general, people seemed baffled by this type of question. There seemed to be a tremendous reliance on mutual trust and a sense of teamwork within the IT organizations we visited. It may be difficult to balance this sense of mutual trust with vigilance against internal risks. Unfortunately, malefactors can take advantage of this.

CHALLENGES IN INSTITUTIONALIZING GOOD SECURITY PRACTICE

A comprehensive understanding of security risks tailored to the environment of your company is only a starting point. Other things are needed to bring about and sustain change in actual practice and behavior in the organization.

Delegation. Because security is the core job focus of only a small number of people, delegation is necessary. Security

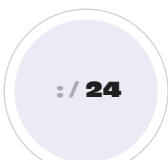
is inherently cross-functional. As a result, it is difficult to fit into the operational chain of command, and must be managed with dotted-line relationships.

Unfortunately, delegation of this sort is difficult. When responsibility is spread through dotted-line structures, task forces, etc., it may be difficult to locate personal ownership and accountability. In the global company, which had a corporate steering committee for IT security, each business unit had a representative who functioned as a conduit between the committee and the business unit. This person was also supposed to take the lead in translating abstract policies into specifics suited to the business unit, and tended to be the local "answer person." However, these responsibilities were add-ons to the person's core job. Thus, they had little impact on that person's rewards and could easily be pushed aside by other priorities.

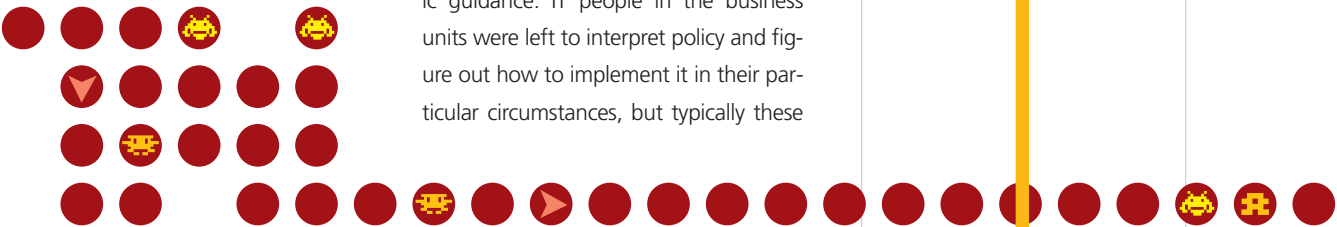
Delegation can have a paradoxical effect of interfering with the institutionalization of security practice by reducing everyone else's investment in the issue. This can be true even—or maybe espe-

cially—if the person receiving the delegation takes a great deal of ownership and becomes a security "champion." We saw examples in which the willingness of one person to take personal ownership seemed to encourage passivity on the part of other IT professionals. Although that person was supposed to influence others, putting security on that person's plate seemed to take it off everyone else's. That person's opinion functioned as *ad hoc* policy. Conversely, if that individual had not yet addressed some issue (which could happen simply because of lack of time or awareness), then others assumed they did not have to be concerned about it.

Finally, dotted-line delegation tends to create a mismatch between responsibility and clout. Success depends on indirect influence, but unless people with direct authority in the reporting structure are held accountable, this indirect influence is often too weak. In one example, managers of departments had been made directly responsible (through their reporting structure) for establishing a disaster-recovery plan. A manager we met with



had mobilized people in his chain of command to address this issue, even pulling them away from their routine work. His whiteboard was covered with flow diagrams representing the process he had developed. In contrast, he was quite disengaged from other security issues, seeming almost unaware of them. His subordinate, who was the local security “contact” in addition to his other responsibilities, had clearly not succeed-



ed in making security a high priority for his manager.

Translating Policy Into Practice.

Another issue that seemed to make institutionalization of security difficult was a gap (both temporal and logical) between development of policy and actual practice in the trenches. The company that had a formal committee to establish security policy provided a good demonstration of this. IT people in the business units complained that there was too long a lag between when someone contacted the committee looking for guidance and when a policy response came back, creating possible risk exposure in the meantime. This temporal gap could be particularly long if the issue were a new one. The policy committee often did not begin work on a new policy issue until a request for guidance came in, because it

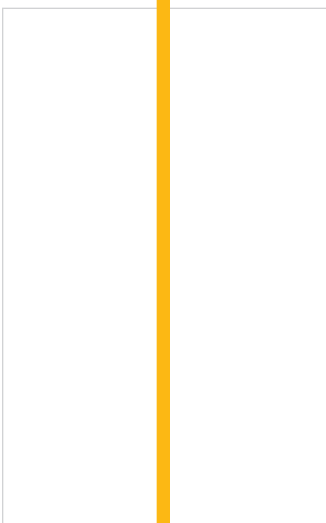
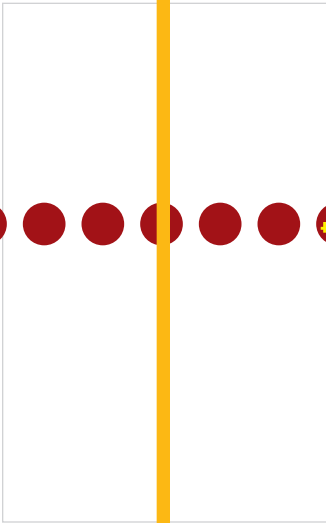
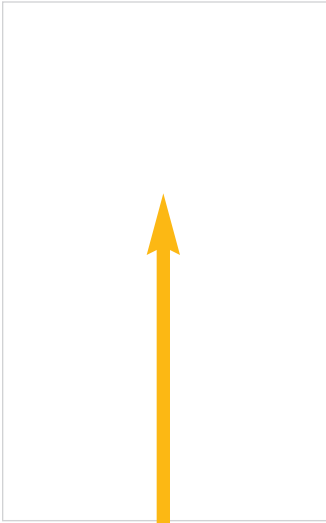
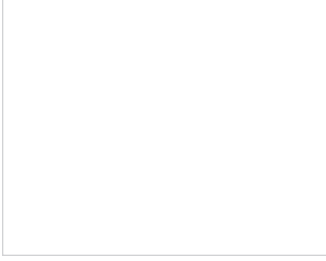
was often through such requests that the committee learned about the issues.

Meanwhile, the logical gap between policy and practice resulted from the fact that the security committee had to write policy to provide guidance to diverse business units that faced diverse challenges and used very different systems. As a result, the policies themselves were written at a fairly high level of generality and often did not give sufficiently specific guidance. IT people in the business units were left to interpret policy and figure out how to implement it in their particular circumstances, but typically these

people were not as professionally focused on security issues as the members of the committee.

Documenting Processes. Even though we know “nobody reads documentation,” it is still hard to institutionalize a technical process unless it is fully documented and the documentation is usable. Without standardized documentation, it is hard to standardize practice, and everything depends on the personal knowledge and habits of individuals or access to the local “security guru.” Lack of documentation makes it difficult or impossible to disseminate information from the small number of people in the organization who focus on the issue to the large number who have a more peripheral role but may be crucially involved in implementation.

Only one of the companies we visit-



ed had made consistent efforts to document security policy, while documenting of procedure was problematic for all of them. Typically, documenting procedure was not a main focus for anyone. Some IT people attempted to do so intermittently, on their own initiative. However, their efforts were informal, and each person invented their own form of documentation. They had little knowledge or training about what makes for effective and usable documentation, or how to compile a usable collection of documented processes. They had no idea if their efforts were

possible to automate patch management and to automate verification of compliance to policy during the log-on process, such as before allowing a laptop that is frequently taken on the road to connect to the network, but they still used manual processes to manage these tasks, walking around to test the machines. The obstacles to setting up more-automated approaches to patching and verifying compliance often had to do with resource limitations. It seemed that the most effective arguments for resources to invest in new tools was not that they would make the company

useful, and what documentation did exist was not routinely updated.

This lack of documentation clearly contributed to a set of problems. We saw and heard of many instances in which action was delayed because of uncertainty about policy, practice, and procedure, and because of overdependence on "oral history."

Automating Security Processes.

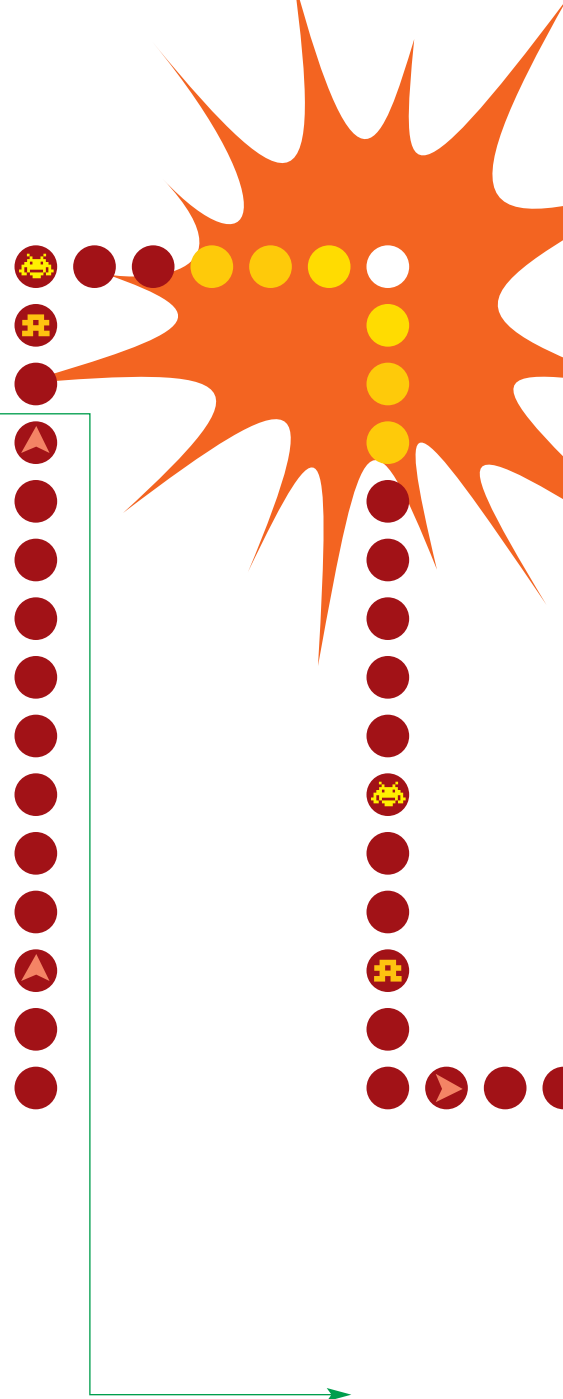
Software tools can potentially help automate processes like deploying patches, verifying the compliance status of machines, and managing permissions, potentially reducing the need to rely on constant human intervention and monitoring for routine things. IT professionals in all of these companies were aware of the possibilities but had made limited progress in implementing them. For instance, they knew it was

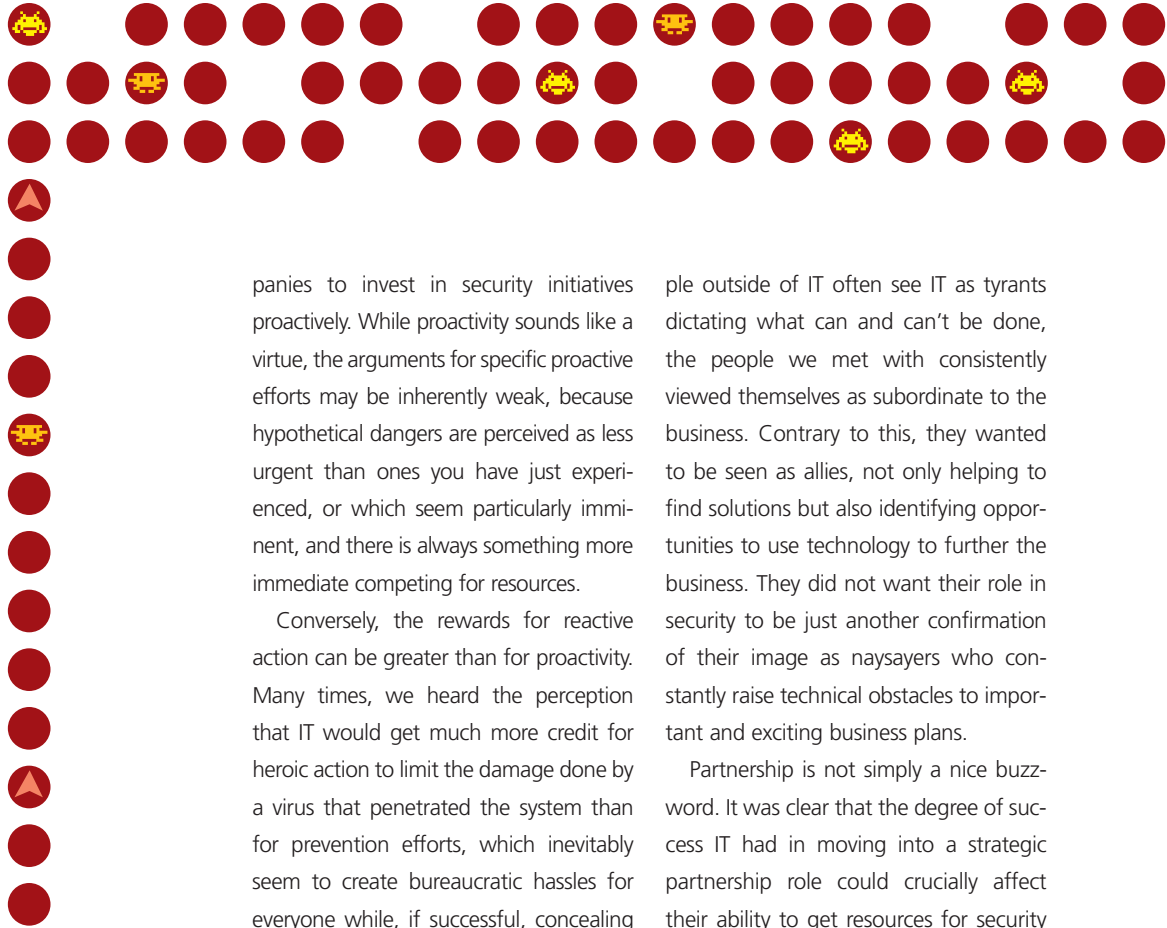
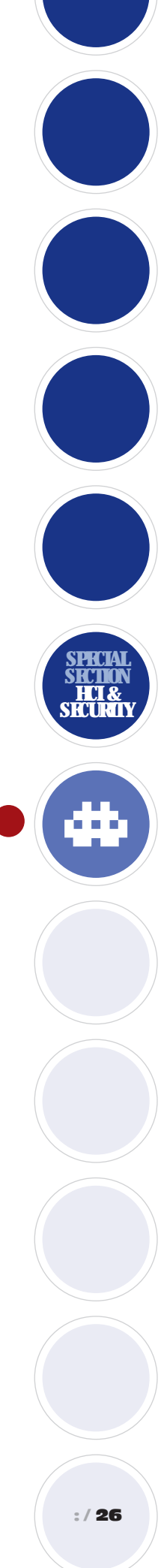
more secure, but that they would increase efficiency of routine processes, like administering permissions.

ORGANIZATIONAL COMMITMENT TO SECURITY

Great technical tools and comprehensive security knowledge do little if IT cannot get the support of the larger organization to make needed investments in the tools and implement practices that impact people outside of IT. In this section, we give a sample of our findings about corporate motivation for security and IT's influence in building this motivation.

The Proactive Versus Reactive Paradox. There is much talk about the need to be more proactive and less reactive in regard to security. However, we heard repeatedly about the difficulty that IT organizations had in getting their com-





panies to invest in security initiatives proactively. While proactivity sounds like a virtue, the arguments for specific proactive efforts may be inherently weak, because hypothetical dangers are perceived as less urgent than ones you have just experienced, or which seem particularly imminent, and there is always something more immediate competing for resources.

Conversely, the rewards for reactive action can be greater than for proactivity. Many times, we heard the perception that IT would get much more credit for heroic action to limit the damage done by a virus that penetrated the system than for prevention efforts, which inevitably seem to create bureaucratic hassles for everyone while, if successful, concealing the real magnitude of the problem.

Experienced incidents were seen as much more powerful in raising the profile of security than information about potential risks. In this sense, although “reactivity” has a negative connotation, it was often an effective way of promoting security as a priority. However, the increased priority typically was not seen as generalizing to other risks. Often, initiatives that are motivated reactively may be too narrowly tied to the most recent event, and not balanced with other needed security strategies.

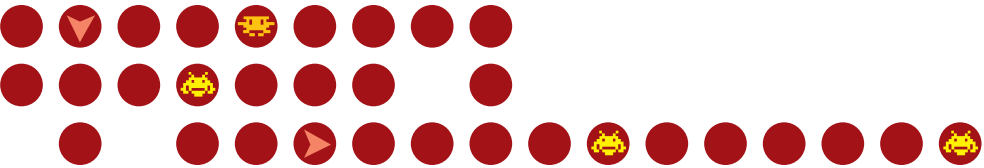
Efforts to Partner With “The Business.” In all of these companies, IT was struggling with how to achieve “partnership” with what they referred to as “the business.” IT people often seemed acutely aware of their limited influence, given their perceived tactical support role in organizations. While peo-

ple outside of IT often see IT as tyrants dictating what can and can’t be done, the people we met with consistently viewed themselves as subordinate to the business. Contrary to this, they wanted to be seen as allies, not only helping to find solutions but also identifying opportunities to use technology to further the business. They did not want their role in security to be just another confirmation of their image as naysayers who constantly raise technical obstacles to important and exciting business plans.

Partnership is not simply a nice buzzword. It was clear that the degree of success IT had in moving into a strategic partnership role could crucially affect their ability to get resources for security initiatives and influence decisions that affect security. One risk of not being in a partnership role is that the business dictates things to IT without recognition either of the resource requirements (both in time and money), or of the potential IT risk exposure that must be managed.

For example, in one company, the business decision had been made (irreversibly and on short notice) to implement functionality on the Web site that could potentially expose the internal customer database to Web-based attacks. The business decision makers almost certainly had not considered this risk, and IT was not at the table when the decision was being made. People in IT felt powerless to influence this decision or the timing of its implementation, or to get needed resources to deal with it.

Some people in IT recognized the existence of natural allies. Corporate finance



people had an interest in security because of their interest in data integrity and were the most frequently mentioned internal allies. Legal people were sometimes cited because of their interest in things like privacy, liability, and protection of intellectual property, although they were also seen as less tuned-in to risks associated with technology. However, note that both of these professional groups also tend to be seen as ancillary to the business, and often share IT's complaints that they are consulted too late. Also, although some IT people talked about working with both of these groups, the focus was always about teaming on isolated projects, rather than building a deeper longstanding alliance around larger issues.

The fact that, in practice, IT security tends to be deconstructed into separate tactical activities (e.g., patch management, anti-virus, firewall, etc.) may contribute to making it peripheral. The narrowly technical and tactical view of security can make it seem like a parochial concern of IT, making it harder to build alliances with a large and influential constituency. Connecting IT security to other risk issues of concern to the business, like financial risk, liability, data integrity and/or privacy might make it clear that IT security is a broader, more strategic-level issue, and might thereby reduce the tendency to pigeonhole it as a low-level function. However, despite their frustrations and desire for allies, there was little evidence that IT people made these links with larger business issues explicit. The very fact that IT

people tended to refer to their internal customers as "the business" seemed to express the sense that IT was somehow separate from "the business."

CONCLUSION

It was very striking how open many people in IT leadership roles were about feeling of out of their element when dealing with the organizational issues that complicate management of IT security. When IT people face such complex organizational challenges, and when they sit across the table from managers from "the business," is it any wonder if IT people do take refuge in focusing in a narrow, tactical way on the technology, which is at least their acknowledged turf?

Unfortunately, as long as IT groups are limited to a tactical support role, IT will continue to have a hard time addressing the organizational issues that impact security. IT security needs to be reframed as an aspect of overall business risk management that happens to be supported through the implementation of technology. Although software and technical processes can be improved and tools can help, IT security cannot be addressed exclusively by technical tools. IT departments are the appropriate home for the necessary technical knowledge and skills, and have the logical vantage point to identify the risks on behalf of the organization, but they also need to own the strategic perspective and the clout to ensure that the organization addresses them in an integrated and effective way.

© ACM 1072-5220/06/0500 \$5.00



ABOUT THE AUTHORS

David Siegel is a user-centered

design consultant who helps companies make their products, systems, and services useful, desirable, and usable. He provides contextual user research, usability studies, and design consultation, and works both in the US and internationally. Until recently, he and Susan co-edited the Business column in this magazine.



Bill Reid is presently director of technology strategy at

Microsoft Corporation. In that role he focuses on the technology needs of businesses ranging from 25 to 1000 employees. Prior to that, he was part of a team that created online informational resources for IT security professionals. He also is a certified information systems security professional.



Susan Dray's consulting firm, Dray & Associates, Inc., has provided user-centered design services to more than 60 clients since 1993. Susan has particular expertise in contextual field research and international user research. She has been a user-centered design professional since 1979 and active in SIGCHI since its inception.