# How Employees in High-Tech Firms Perceive Cyber Security

**Erin M. Fitzgibbons, Alex A. Khadiwala, Carlos D. Rodriguez, Weiwei Yu**
fitzgibb@colorado.edu, alex@khadiwala.com,
carlos.d.rodriguez@colorado.edu, weiwei.yu@colorado.edu

A capstone paper submitted as partial fulfillment of the requirements for the degree of Masters in Interdisciplinary Telecommunications at the University of Colorado, Boulder, May 2, 2003. Project directed by Professor Tom Lookabaugh.

## 1. Introduction

This paper examines the balance between innovation and the electronic security measures and policies designed, implemented, and enforced to protect high-tech companies' sensitive data. To what extent do these security measures and policies, ostensibly protecting sensitive data, interfere with innovation and invention within the company?

This is a topic that is foremost on the minds of a wide range of people, from engineers, who are concerned with how security can interfere with their innovation and work efficiency, to information technology (IT) employees, who are concerned with protecting the company's network. And finally we have upper management, who is interested in the bottom line with respect to protecting their competitive advantages and keeping their resource expenditures at a minimum. Most of the research on IT security has focused on the technical aspects while not touching much on human interaction with security; as a result, implemented security systems may not run as smoothly or effectively as planned. We believe that there are often tradeoffs between a corporation's IT security and its employees' ability to perform the tasks that increase its competitiveness and longevity in the marketplace; we will examine the intricacies of these tradeoffs to start a process of determining how better to mesh current and future implementations of corporate security.

## 2. Relevance to Prior Work

Technological advancements have revolutionized the way in which people communicate and do business. Being connected to some sort of network in which information is exchanged has become an essential part of most professionals daily work regime, especially in the high tech field. Advances in communications technology also have brought on the need for establishing security to protect the valuable information that may be stored or transmitted between employees. Much like the Internet itself, the roots of computer security began under the control in the US military, in which users were expected to obey the security rules in place [4]. Realizing that the military environment was not exactly typical of most business organizations, "with skilled, empowered knowledge workers, who do not work under constant supervision and are supposed to use their own initiative," Bell and LaPadula (1976) developed more general security models that could be applied to an array of secure systems [4] [8]. The security community continued to explore possible security models and security in general. Many aspects of security were surveyed, including how to define technical requirements for secure systems and their corresponding rules of operations [8]. As this old perspective on security continued to evolve, however, the industry continued to focus on the technical aspects of security, such as encryption and firewalls, while ignoring the human factor [3] [7].

It was not until recent years that the security community began to acknowledge that user behavior often contributes to many security failures, and thus, began considering the effects of human factors on security [2] [3] [4] [6] [7]. Some of the researchers that have been at the forefront of investigating this human component include M. A. Sasse, Dirk Weirich, and Helen James. The majority of the work that they have done has revolved around password mechanisms and ways to persuade users to comply with security [2] [3] [4] [6] [7]. Our study examines how individuals (research and development engineers) working in two medium-sized high-tech firms perceive security in comparison to how the Chief Financial Officers (CFOs) and IT directors perceive it. Research and development engineers were chosen because we believe they have a strong need for flexibility so that they can be as creative and productive as possible. Similar to the research done by Parker, in 1997, our work also attempts to explore the constraints of security, but in relation to research and development engineers [5]. It is our intent that our results will help to design computer security policies that reflect the costs of security in terms of productivity and innovation, thus resulting in more effective and logical implementation of future policies.

## 3. Methodology

Semi-structured interviews were conducted with employees of two medium sized high-tech companies, Company A and Company B. Company A has roughly 180 employees of which 11were interviewed, all being engineers with the exception of the CFO, Network Administrator, and Director of IT. Company B has roughly 350 employees of which 7 were interviewed, all being engineers with the exception to the CFO and Director of IT. The intent of interviewing two companies was to gain a better understanding of the data through comparing the results from each data set. The interview questions pertained to how each user interacts with security, what effects security has on their work, and how they value security. Semi-structured interviews were chosen as our interview method, as they would not constrain employees' answers, instead it would allow them to divulge details or anecdotes that may come to mind in the course of an interview. The foundation of the semi-structured interviews is based on the conceptual research technique known as Grounded Theory [7].

Compared to grounded theory, quantitative research is misrepresentative of reality due to the inherent constraint of the questions: the data gathered is based on the questions asked. In addition, how does one know specifically what questions to ask? Meanwhile, purely qualitative research lacks the objectivity necessary to make concrete arguments. Grounded theory is a compromise between quantitative and qualitative research. Semi-structured interviews were performed and all conversations were recorded, transcribed, then analyzed using a technique called coding. Coding is performed by reading through the transcribed conversations and highlighting key concepts pertaining to the subject matter. To help remove bias and help extract more consistent information, each interview was coded by two different researchers. Through coding, a researcher can begin to connect similar concepts between different interviews, and start building theories Thus grounded theory is qualitative due to the interview process, but shares some aspects of quantitative research through the objective analysis of the coding process. Through this methodology of research, six main concepts were identified, and shall be discussed in more detail through the remainder of this paper:

- Preference for security to be invisible
- Users are unsure of proper procedures when dealing with security - variance of "common sense" security practices
- Perceptions vary based on job-specific goals
- Lower security precaution adherence as a result of trust among employees
- Lower security priority as a result of the perception of a low company profile
- Lower security priority as a result of reduced resources

## 4. Analysis

It is important to state that both Companies A and B are relatively small and their reputations and brands are limited to a particular industry segment. Additionally, both companies do not have explicit security policies and they do not provide training in regard to security issues. Finally, it also necessary to state that the employees interviewed at Company B worked in a start-up environment before their business merged with the Company B.

### 4.1 Preference for Security to be Invisible

Initially it was surprising to find that many of the R&D engineers lacked knowledge about the security technologies or practices in place within their organizations, but after many interviews were conducted we found that it was due to a lack in security policies, and the invisibility of the security that was in place. Interestingly, this coincides with the employees preference of having security be invisible. "I think security is important to me, but I'd rather it be someone else's job," stated an employee from Company A. When an employee from Company B was asked of their view on security, they remarked "I'm insulated from that. I don't know anything about it. I feel I'm fine." Interviewees seemed to have a certain level of comfort with security, even though they may not know much about it.

Invisible security does have its consequences, however. When asked if the network at Company B was secure enough, an interviewee stated, "If I started thinking about security and being concerned about it, then I would suggest changes." Thus, this invisibility seems to create a lack of motivation among engineers and their attitudes towards security. When first contacted to request interviews for our topic, most interviewees researched whether or not their company had a security policy, and if so what it included. Consequently, by just mentioning security to these employees we were able to motivate them to at least know what policies or guidelines exist within their organization. Furthermore, invisible security has the potential of compelling employees to make their own assumptions regarding security.

### 4.2 Users are Unsure of Proper Procedures when Dealing with Security - Variance of "Common Sense" Security Practices

As both Companies A and B lack explicit security policies and training pertaining to security issues, the employees themselves are left to decide right and wrong. Almost every interviewee stated an instance in which they were unsure of how a particular action or behavior affected security. One Company A employee who sends sensitive work data to his personal email account stated, "I don't know if I am doing the right thing when I do that." In contrast, an employee of Company B spoke of how file-sharing is prohibited in his company, even though it is not explicitly stated, "It's kind of an obvious thing." These employees have different perspectives on security, and because there is no detailed documentation from their employers on proper security procedures, their past experiences and "common sense" dictate how they work. Similarly, past experiences affect their behaviors and views on security. People who worked in very secure environments, such as the Department of Defense, were accustomed to a more security-minded environment as compared to those who worked at a more relaxed environment, such as a start-up. An employee of Company B stated, "I used to work in aerospace 10 years ago and you had to worry about security a lot more." Another employee of Company B who came from a startup company with little security stated, "I tend to have a startup mentality, it's just like 'just do it, don't worry about the details, just do it. Make things as simple as possible.'"

### 4.3 Perceptions Vary based on Job-Specific Goals

Just as perceptions concerning security vary by the type of experience or background an employee has, we also found that they vary by the particular job title an employee holds as a result of their job-specific goals. Beginning with the CFOs of both companies, they seemed to know *about* security, but on a higher-level. Neither CFO could talk about the specifics of the security technology in place at their organizations because it did not have a direct effect on their goals. The CFO at Company A stated, "It's not building a new product, it's not decreasing an expense, and right now that's what we're trying to do, reduce expenses." Thus, his goal is not to be completely informed on the ins and outs of security and all the possible vulnerabilities that may exist, rather his goal is to be watchful of company expenditures. The CFOs did not under prioritize security, however, given that one of their goals includes providing and protecting their company's financial data. "In the finance world security is very important because we have financial information and payroll information on the network," said one CFO when speaking about the importance of safeguarding data. A loose security policy could possibly compromise such important documents, thus security is on their minds.

In contrast, the Information Technology (IT) directors were much more informed and concerned about security because it directly affects their job-specific goals of ensuring reliable network technology and communications. IT directors at both companies take the extra time to inform themselves on current security issues or technologies by reading articles on the Internet or subscribing to specific journals. Whereas the CFOs' knowledge of security was more superficial, IT directors spend a great deal of time considering the tradeoffs of implementing and maintaining security measures. One IT director stated, "Security is one of those things that like it or not, you end up treating it as somewhat of an optional thing…unless you end up with a crisis." Even though security may be treated as "optional" it appears to become something that is regularly discussed. Sometimes a decision not to implement security can have a disastrous effect on an IT director's goal of providing fast service to the organization. "I can't tell you how many fire drills we have gone into because some virus gets in here, and all the sudden you drop everything you are doing and you fight a virus for a day or two…it's a huge waste of time," said one IT director. The decision to implement security or not is always on an IT director's mind. Ultimately, the IT director must balance network security and other IT-related tasks, given finite resources.

Finally, the R&D engineers' perceptions of security seemed to be the most simple. Whereas the other types of employees had some direct ties to security and their goals, most of the engineers perceived security as simply the five seconds it took them to enter their password in the morning. One engineer, when speaking about his current company in comparison to a previous place of employment where security was more rigid, said "Here, I feel like I spend more time writing software." The goals of R&D engineers include being creative, and above all else, being productive, and the five second "security encounter" did not have much of an effect on those goals.

### 4.4 Lower Security Precaution Adherence as a Result of Trust Among Employees

When speaking with employees from both Companies A and B, a sense of trust was strongly conveyed in many of their responses. Many employees seemed to feel that their small organizations created environments where trust could flourish and thus strict control was not necessary. The actions and behaviors based on this trust for their co-workers, however, sometimes inadvertently lead to security compromises relative to external threats.

The IT director at Company B had much to say about trust among peers. "We rely a whole lot on the people that we have working here. We rely on trusting them, but you know that has its limitations too." Company B recently laid-off an IT employee. They carried out the common security practices, such as not indicating his pending layoff in any electronic messages beforehand, as well as disabling his account when the time came to lay him off. After auditing his actions and files, they discovered he had been looking at things he had no legitimate reason to see, such as Human Resource (HR) information. This employee had betrayed the trust placed in him. Of the current email administrator, however, Company B's IT director says "he is not that kind of person.

And those are the kind of people that you look for, for those positions. If people don’t have integrity, it does not matter what you do to secure a network.”

The IT director indicated that they also have to trust that people are not walking off with hard copies of sensitive data, whether in the form of print-outs, burned CD-Rs, floppy disks, or USB-enabled compact flash cards. In order to prevent that, these devices would have to be removed from every computer, but that would hinder innovation.

> *It’s not a very controlled environment. In a really controlled environment, you can say, ‘at this machine this is the only person besides an administrator who can sign in.’ We don’t do that. That would stifle creativity. People like to move around, especially in engineering lab. They like to go to a machine and log into it. And you sometimes just have to accept the fact that if engineers want to do something, we let them do it. They are big boys and girls and they take care of themselves, and when they get into trouble they are on their own. We give the engineers more leeway than anybody else; they are the core of this company.*

The IT director from Company A said that in order to concentrate on keeping malicious outsiders from doing damage, they have to trust their own employees until they are given reason not to. In fact, he said that they may be a little too open in some ways – very sensitive places like networked HR or Finance folders and databases are restricted, but that is the extent of the restricted items. Since they are such a small company, they cannot afford to put roadblocks in the engineers’ way; they have to trust them to manage certain responsibilities on their own, such as fixing servers or databases. Non-engineers do not receive as much trust with respect to network access.

He went on to recount his experience in more restrictive companies, where employees had to ask permission to do anything, and receiving this permission often took too long. In contrast, Company A’s IT director gives its employees enough trust to allow them to get their jobs done. “The moment you start throwing rules in somebody’s face they are immediately going to want to break them. It’s human nature. If you give it to them based on the honor system, they have fewer tendencies to go out and break them.”

Both companies have experienced layoffs recently, but the perceptions regarding the laid off workers were much different than we had expected. One employee suggested that in terms of trust with employees leaving the company, there is an expectation of overall good conduct, in that the last thing a laid-off engineer would want to do is “burn bridges” that would adversely affect his chances of getting hired at another company. Our data supported the fact that many engineers viewed their field as a tight-knit community, in which people’s career paths always seem to cross. As a result of the shared trust, employees did not seem to leave with a bitter mindset.

All of the engineers from Company B came from a startup, and thus were accustomed to an open and less secure working environment. One engineer noted that during late work nights he would find workstations unlocked, at the same time custodians would be busy cleaning the office. “You have no idea in the 2 hours when they keep all the doors open for cleaning, who’s been in and out.” This engineer said that while he is not too strict about security, he felt that the lackadaisical mindset of the startup engineer carried over too far into Company B; unlocked doors make sabotage easy, and you would not know who did it or when it happened. An engineer from Company A echoed his concern, citing the need for automatically locking workstations and the frequently mentioned example of after-hours custodians using open company workstations to access pornography on the Internet. This employee believes that the security policy must be more proactive, that "you can't just sit on the sidelines and wait for a fire to start… that's just too late." He said that the order for more proactive security must come from the top so that everybody is made aware of what the policies are and so that everybody follows through.

Another example of security is compromised in order to enhance productivity, engineers at Company B use a common password to access lab computers. In case anybody forgets it, the password is conveniently written on the dry-erase board, and the computers are left logged in all the time. Of trust and security, another engineer in Company B says "we in engineering like to leave things fairly unprotected so we can go and access other people's directories so if the people I'm working with are changing files, I can work with their latest revisions." An engineer in Company A expressed, trust does not always imply carelessness:

> *Personally I choose to believe that I work with people I trust. I heard a story of someone who was working with a well known telecommunications company with some immature coworkers. If you didn't lock your workstation people would send email from your computer to the CEO saying stupid things. Maybe I choose to believe, maybe erroneously, that I work with people more mature than that, but things like that could happen, and if it did happen I would be more careful. Should I be more careful? Maybe. I think it's needed for those few instances when people will want to do something, but I probably feel comfortable, as far as my co-workers are concerned, just walking away, leaving my stuff open.*

The CFO of Company A is a little less trusting; he has set his computer to lock after a short period of inactivity. "Right now my door is open and I don't need people going in and seeing what emails I sent." The CFO and an engineer recounted the same instance where a person in a position of trust betrayed that trust. This person, the company's email administrator, was reading an executive's email. This was discovered because he consistently knew information that he should not have known. He was fired shortly after this discovery.

### 4.5 Lower Security Priority as a Result of the Perception of a Low Corporate Profile

There was not one person in either company that felt his company was a high-profile "target" of internal or external hackers. This perception results in security becoming a lower priority, a function that does not even have a specific budget. The rhetorical question many people asked was "what is the probability that anybody will care enough to target our company's network with a serious attack?"

Many employees cited the fact that compared to a high-visibility commercial company or Department of Defense contractor; their respective companies were low profile. For reference on relative visibilities of the two companies, a *Google* search showed IBM has approximately one hundred times as many results as Company B, which has approximately five times as many results as Company A. As an engineer at Company B said:

> *I don't think of this being a high security place. I don't think there are people trying to steal our secrets. I don't really worry about that too much. My feeling is that we should be relatively loose around here. It's all relative though, it depends on who is doing the thinking here, this is all from my point of view, but if there were more important secrets, then there should be more important policies, and they should be enforced more strongly. It is a compromise.*

### 4.6 Lower Security Priority as a Result of Reduced Resources

With respect to reduced security resources, the IT director from Company B said:

> *We talk about ways of improving security, but often they fall by the way-side when more pressing issues come up. Could we improve security? If we could live in a perfect world, you bet. If we had one cutting edge system with an army of people to keep it in top shape, that would be great. And even then, you see that the places that do have things like that still wind up with security problems. Even a place like Carnegie Mellon's CERT, known for its top-rate network security, is at risk from internal attacks; recently someone internally compromised their network. A lot of our security measures are comprised of convincing the engineers to adhere to better security practices.*

The CFO from company A agrees: "It's easy to say there are ways the company's network can be better secured, but it's kind of hard to put one in place, especially when you are 30% of the size you were before, trying to do the same amount of work."

At one point Company B was supported by a group of 70 IT professionals; now there are 17 supporting the same network. The IT Director says that there is always a tradeoff between productivity and security, and unless there is an army of people supporting the engineers, the IT department has to step back and let them take care of themselves to a certain extent.

An interesting finding from the IT director from Company A is that with tightening security with respect to passwords, which typically means increasing the frequency at which they must be changed, the IT department comes under a lot of strain with employees calling in for help because they forgot their recent password iteration.

> *The problem with changing passwords is people forget them, so you are constantly resetting them or people are writing them down if you change them all the time. It's a constant support problem. We're spending lots of time with people who are constantly forgetting their passwords. So we've kind of just let it be and haven't gone any further with it at this point. I haven't decided what to do. The tendency of our CEO is to go more towards the secure and make everybody change it. But then we'll just get a*

> *lot more support calls and people will start writing them down instead of using the one they like and remember.*

## 5. Conclusion

### 5.1 Factual Conclusions

It is a plain and simple fact that a completely secure organization does not exist. If such an organization were to exist, it would be certain that the limitations placed on its employees would severely affect their productivity. Thus, there is always a tradeoff between how secure an organization is and the extent to which its employees are free to perform their respective jobs. The overall themes that were identified through our interviews include:

- Security tends to be invisible. This creates a lack of awareness which leads to employees having low motivation towards security procedures.

- Lack of explicit security policies and communication leads employees to draw upon their own past experiences and what they believe to be "common sense" when interacting with security.

- Employee's perceptions of security vary based on their job-specific goals; security is only on their mind if it is going to affect their job activities.

- The relatively small size of both organizations lends for a strong sense of camaraderie and trust amongst employees, and especially within given groups (e.g. R&D engineers). This trust allows for a lax enforcement of security.

- Employees placed a low priority on security because they perceive their organizations as having a low corporate profile, and thus information that is not highly sensitive.

- Those responsible of making decisions on security issues place a low priority on security due to the limited availability of financial and human resources (e.g. budget and "manpower").

We are obliged to say that our conclusions may appear obvious, but most security policies and practices apparently ignore or can not address these findings, suggesting that anecdotal and "common sense" understandings need to be addressed by documented and careful research if we are to actually deal with the overall security outcome in organizations.

### 5.2 Suggestions for Further Research

Given that the precedence of research done on the human factor of cyber security has revolved around the ways in which security is violated and the methods of enforcing certain "secure" behaviors, our research has taken a step back to see how employees actually perceive the security that is in place. Overall, it did not seem as if employees at either organization felt constrained in their everyday tasks, nevertheless, we are wary that this would not be the case had different types of organizations been researched. We hope that our research provides a framework for exploring other types of organizations in the future, eventually leading to a comprehensive guide on human interaction with cyber security in an array of organizational structures. Some of the types of organizations that we would suggest be researched include those that have a much stricter cyber security policy in place, those that are larger in size or those that have a higher corporate profile. It would be useful to the security community to compare the themes that result from more research in order to develop policies that create a sense of balance between an employee's ability to innovate and their productivity.

## References

[1] Adams, Anne, and Martina Sasse, "Users Are Not the Enemy," Communications of the ACM, Dec. 1999, Vol. 42, No. 12, pp. 41-46.

[2] Brostoff, S., Sasse, M.A., and D. Werich, "Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security," BT Technol J, Vol. 19, No. 3, July 2001, pp. 122-131.

[3] Dobson, John, "New Security Paradigms: What Other Concepts Do We Need as Well?," Proceedings of the 2001 workshop on New Security Paradigms, 2001, Cloudcroft, New Mexico, pp. 7-18.

[4] James, Helen, "Managing Information Systems Security: A Soft Approach," Proceedings of the Information Systems Conference of New Zealand, Oct 30-31, 1996, pp. 10-20.

[5] Parker, Donn B., "The Strategic Values of Information Security in Business," Computers and Security, Vol. 16, No. 7, 1997, pp. 572-582.

[6] Sasse, Martina and Dirk Weirich, "Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World," Proceedings of the 2001 workshop on New Security Paradigms, 2001, Cloudcroft, New Mexico, pp. 137-149.

[7] Strauss, Anselm, and Juliet Corbin, Basics of Qualitative Research. Thousand Oaks: Sage Publications, 1998.

[8] Strens, Ros and John Dobson, "How Responsibility Modeling Leads to Security Requirements," Proceedings of the 1992-1993 workshop on New Security Paradigms, 1993, Little Compton, Rhode Island, pp. 143-149.