

Good Intentions, InfoSec Policy and Ethics - A Case Study

By John Thompson, University of Iowa

45

I have been a system administrator now for a number of years. During the early years of my tenure as a system administrator, I did not know much about security and, frankly, could not have cared less. There were too many things to do in precious little time; doing anything for security seemed like a waste of time. I left most system settings the way they were when I installed systems. I hardly ever looked at audit logs. I never asked questions such as whether user accounts were still active or dormant. I was in many respects a very typical system administrator.

The Scenario

Things stayed this way until a little over a year ago when I met an information security professional who got me interested in security. He told me about measures I would have to take to tighten the security of the systems I administered and why I might want to consider doing so. He told me about web sites and books that could help me learn more about security. I even attended a security conference and sat in on a number of excellent tutorials designed for system administrators who wanted to secure their systems.

I decided to go to pursue university studies and, after being accepted, determined to apply for a system administrator job at the university I would attend. Shortly after I arrived, I interviewed for this position and was hired. I was ecstatic. I had a reasonable amount of experience as a system administrator, meaning that I would not have to constantly be in learning mode. This very likely would leave me with more time to pursue my studies. But I also realized that with what I now knew about security, I could make a genuine difference at the university. After all, universities are renowned for notoriously poor information security. My being a conscientious system administrator would allow me to help my university avoid the negative reputation that other universities suffer. At least so I thought.

I spent the first few days on the job learning my responsibilities. I also wanted to impress my supervisor and others within the department in which I worked by letting them know that I did my work thoroughly. I was willing to go above and beyond the normal duties of someone in my position. When I told my supervisor that I had

been learning security, he seemed enthusiastic. I told him that I could make our systems considerably more secure than they were at this time, and I distinctly remember his giving his approval.

Off I went on my security crusade. I started by scanning what I had been told was our department's web server with a port scanning tool. I understood that this server had been left unattended since the last person in my position had left the department. With great eagerness I launched a port scan to identify open ports on this system. Shortly afterwards I found port 12345 to be open. This indicated that a copy of the notorious netbus¹ Trojan horse program was running on this system. I could hardly believe it - the first system that I scanned had a malicious tool running on it! But I wanted to be sure before raising any kind of alarm - after all, I was new at the university. I remembered that one way to remotely connect to netbus was to remotely use a client version of netbus, directing the client to the netbus server. I did this - netbus connected without a password. I verified conclusively that the Trojan program was indeed netbus and not some other program that was running on the web server that utilized the particular port in question. I hadn't done very much, and I already had a very important finding to report. I felt a sense of pride in the learning and my work ethic that had brought me to this place.

Why was the copy of netbus on the web server, anyway? Obviously, I thought to myself, it was not there for administrative purposes. A sense of intrigue overcame me as I imagined how some attacker might have planted this program. Then I suddenly realized that although I had found this insidious program, no one else might even believe me, or even if so, would not be likely to care. I remembered when the last lead system administrator for whom I worked had said: "Until you find a hole where you can access my files, I don't care." I felt obliged to show proof, so I took screen shots and copied a text log. I also enabled password protection on the web server and set up email notification so that it would let me know the next time someone attempted to connect.

¹Netbus is a Trojan horse program that, once installed in Windows NT systems, allows a remote user to gain remote control of the system in which it is planted.

The next day I was still bursting with enthusiasm. I wrote a detailed incident report and submitted it to my supervisor during our meeting that day. I was pleased with his reaction. He was ostensibly alarmed; the fact that he notified the department's computing committee indicated that he intended to investigate this matter further. The committee convened shortly afterwards. They had me debrief them concerning how I found the Trojan, how it worked, and the outcomes that could occur. The committee members seemed excited and determined that my report should go to the dean of the college and to our department head.

The euphoria that I experienced did not last long, however. I soon learned during the meeting with the department computing committee that the web site in question was hosted on a system operated by the college in which our department belonged. Our department thus did not have jurisdiction over this system. I then requested that they contact the system administrator of that system first. They later elected instead to send e-mail to faculty and staff within the college. From that point on I do not know exactly what happened, but the dean of the college was apparently unhappy that someone had installed a Trojan horse program on one of the college's servers. Eventually the news got back to the administrator of that web server. The next thing I knew, this administrator accused me of unauthorized access to this system. He threatened me with prosecution and expulsion from the university. A week went by while he met with the committee and department head without my being allowed to be present.

I requested to speak with the system administrator who had accused me. The department head set up a meeting and attended it in support of me. The meeting began with small talk, but it didn't calm me down. I was nervous. When I asked him what he planned to do, he said that he was going to try to get me fired from my job, then expelled from the university, and possibly prosecuted in a court of law. I took a deep breath, then began to stand up for what I did in a professional manner, trying to be careful to avoid making the situation worse. This system administrator attacked me from several angles, while at the same time attempting to find a loophole in my story. He informed me that the university had a security policy and questioned me why I had not adhered to this policy. Next he asked me if I had ever compromised systems before. He posed additional incriminating questions, then started bringing up personal information that he had apparently found in my university records (such as recommendations that others had written for me). This struck me as com-

pletely inappropriate²; I requested that he stick to the facts relevant to the issue.

The final outcome was not as bad as it could have been. Soon afterwards the system administrator found that I had been misinformed about the ownership of the web server. He also learned that I had been told that there was no network security policy in place, so I didn't know that I was violating it by scanning for open ports and Trojan horse programs. In the long run, nothing came of all of his and the others' rhetoric. I was allowed to remain enrolled at the university; I did not lose my job as system administrator. Later I learned that he and others had been posturing in a manner designed to appease the head of the college (and possibly also to avoid being blamed for negligence in allowing one of their systems to be compromised by a Trojan horse program).

Lessons Learned

Once the trauma of this experience began to subside, I was able to more objectively evaluate what I had been through and to discover lessons learned. To my amazement, I found that what I experienced was not all that atypical - that many others like myself have undergone similar experiences, sometimes with better, sometimes with worse results. I learned, for example, of the story of Randal Schwartz, contractor to Intel in Portland, Oregon, USA. As a system administrator concerned with security, he engaged in actions such as remotely copying the password file of a system to another. One of his primary purposes was to prove that security had deteriorated since he left one organization within Intel for another. He was ultimately accused of wrongdoing, then tried in a court of law and convicted of three felony counts in Oregon (SCHW00). He not only accrued massive financial debt for his legal defense, but his being convicted of crimes has damaged his employability. I also learned that many years previously, Oregon (in addition to many other Western USA states) had passed little known but very strict laws concerning computer crime in response to lobbyist pressure from a telecommunications company.

I had been relatively fortunate; Randal Schwartz had not. Yet the Randal Schwartz case and mine have many elements in common.

My experience has taught me several important lessons:

1. Small actions on the part of a system administrator can have major consequences in terms of the system administrator's continued employment and the law. What seems small to a system administrator may not in reality turn out to be small in terms of repercussions. Typical system administrators really have no way of knowing what the relationship between system administrator ac-

²The fact that a system administrator could gain access to student records in this manner raises serious ethical and privacy concerns.

tions and consequences when they start a job. System administration thus poses much higher occupational and legal risk to the system administrator than one might imagine.

2. Employers are in the best position to address the previously mentioned problem. By indoctrinating all employees who will use computers concerning restrictions that apply to usage, they do their employees (especially system administrators) a big favor. To leave employees uninformed is not only unethical (because of all the problems that real and suspected misuse can cause for employees), but it also can lead to massive legal problems and public image damage for corporations and institutions that fail to do so. System administrators as well as other employees, especially those with an inclination to improve security, can readily get themselves in trouble by doing what they believe is correct on the basis of their previous job experience and other learning. I urge all organizations, no matter what the emphasis on information security may be, to prepare a statement of accountability that covers who can use which particular systems with what particular levels of privilege. It should also explain what employees and contractors are not allowed to do when they access systems (BERN96). Employees should be required read and sign this statement when they commence employment, and also at frequent (e.g., one year) intervals.
3. Employees, especially system administrators, should invest a good amount of time to discover the actions that are and are not permissible from the employer's or client's perspective. It is important to never assume that what one does in the name of security will be acceptable to an employer or client. As the saying goes: "The road to hell is paved with good intentions."
4. Anyone who does work in the name of security should obtain explicit, written approval before initiating any kind of activity that resembles an attack or something that may otherwise be considered unauthorized. Make sure that this approval specifically covers the planned security-related or other activities. Some management is good, some is bad, but few managers will stand up for accused employees when the manager's job could be at stake if the blame cannot clearly be placed on the accused. Obtaining advance, written approval to perform potentially controversial tasks is the only survival strategy for employees and consultants or contractors who engage in activity such as penetration testing and vulnerability analysis.
5. Learn the security culture of your organization first before attempting to take action that improves security. Even if someone val-

ues security highly, being the only one who cares about security and wants to adopt appropriate measures potentially puts that person in an extremely precarious position. Doing something about security when others in an organization do not really care about security is dangerous from a professional as well as a legal perspective. It would be better to attempt to interest a few others in one's organization in improving security and, eventually, to enlist their support in undertaking measures that elevate security, rather than to be the one employee who is perceived as "out of line." Put simply, zealots for security get in trouble.

Aftermath

I still work at the same job at the same university. The experience I had, however, dramatically changed my perspective about information security. For one thing, I now have the suspicion that someone such as myself almost certainly previously tried to change security for the better at the same university I attend and ended up suffering through the same outcome I did. I am also now considerably more inclined to do only the minimum for security - to adopt the measures that are least likely to cause trouble. Is it any wonder, then, that universities are known for their deficient information security? I suspect that the same principle applies (at least to some extent) to commercial and government enterprises and government agencies. Unless clear and explicit support for doing security-related tasks is given to system administrators, the system administrators, the first line of defense in any organization, will not get the job of properly securing systems and networks done.

But above all, this whole experience brings up another question related to ethics. Why are employers so quick to accuse, but negligent to inform users of the ground rules? Why are conscientious system administrators threatened with legal action in cases such as mine, when literally thousands of attackers access organizations' computers without authorization, but little or no attempt is made to track their actions, let alone make them face the consequences of their actions? Why are antagonistic system administrators allowed access to personal information? These and other critical issues desperately need resolution. Until some kind of satisfactory resolution occurs, cases such as Randal Schwartz's and mine will continue to occur. Everyone loses in these cases.

References

- BERN96 - Bernstein, T., Bhimani, A., Schultz, E., and Siegel, C. (1996) *Internet Security for Business*. New York: Wiley.
- SCHW00 - Schwartz, R. (2000), *What Do We Have to Learn from the Randal Schwartz Situa-*

SYSTEM ADMINISTRATION

tion? In Proceedings of Spring 2000 Joint Computer Security Conference.



John Thompson is a Network Administrator at the University of Iowa. In this role, he takes care of the computing needs in his department including securing systems, providing technical support and maintaining their web and file server.

Before working for the University of Iowa, John was a Web Programmer for Dynamic Systems Solution Group, where he also began his training as a Network Administrator. After working for Dynamic Systems, he was a Research Associate for the SANS Institute. John is currently a freshman at the University of Iowa majoring in MIS and Computer Science.
