

8

IT Security Program Success: What Matters

Security is a negative deliverable. You don't know when you have it. You only know when you've lost it.

—Jeffrey I. Schiller

In this chapter we describe the perceived level of success information technology (IT) security programs have attained at our institutions and discuss factors that contribute positively and negatively to their success. Included are technologies in use, staff experience, institutional size, the organization of campus IT security, the presence of policies and IT security plans, awareness programs, and budget.

How Successful Are We?

We used a Likert scale ranging from 1 to 5 (1 is strongly agree, 2 is agree, 3 is neutral, 4 is disagree, and 5 is strongly disagree) to assess each respondent's opinion on the success of his or her institution's IT security programs and on benchmarks for success. We asked five questions:

- ◆ How would you characterize your program's success?
- ◆ Has your institution gone beyond federal and state government IT security requirements?
- ◆ Are data, networks, and applications that are your responsibility secure?
- ◆ Have you developed metrics to determine IT security activities' effectiveness?

- ◆ Is your institution more secure today than it was two years ago?

We calculated the mean for each question and then compared the means by Carnegie class, along with a category for Canadian institutions (see Table 8-1).

The respondents were most positive about feeling more secure today than two years ago despite being in what we perceive as a riskier environment. The mean of 1.86 shows that a majority agreed or strongly agreed that their institutions were more secure today. The next most positive response was to the question, "How would you characterize the success of your IT security program?," with a mean for all of 2.40. We found little difference on any of the questions by Carnegie class, number of devices and users, or country.

What our respondents appear to be telling us is that they feel more secure today, but their IT security programs still need strengthening. Interestingly, when we asked respondents individually about the data, networks, and applications they were responsible for, the answers were less positive, though still positive overall. Most respondents felt that they had not gone beyond state and federal requirements, nor

Table 8-1. IT Security Outcomes, by Carnegie Class

Carnegie Class	Program Is Successful	Beyond Requirements	Systems Are Secure	Metrics Developed	More Secure than Two Years Ago
Dr. Ext.	2.32	3.27	2.78	3.42	1.78
Dr. Int.	2.35	3.21	2.74	3.44	1.83
MA	2.31	3.49	2.79	3.68	1.95
BA	2.35	3.28	2.53	3.60	1.84
AA	2.27	2.98	2.46	3.28	1.77
Specialized	2.34	3.25	2.65	3.47	1.89
System	2.31	3.06	3.00	3.52	2.00
Canada	2.40	3.44	2.76	3.67	1.95
All Respondents	2.31	3.28	2.68	3.52	1.86

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

had they developed metrics to determine their IT security programs' effectiveness. So, for the most part, assessing the security level remains, for many institutions in our survey, a subjective exercise.

The people we interviewed had varying opinions about what constituted success. Bruce Judd, associate vice president at San Jose State University, stated, "Success is measured by the number of problems we have. When I look at the number of problems we had a year ago and the number of problems we have today, the reduction is dramatic. I feel that we have been successful in reducing the number of incidents, but it is not as successful as we could be and where we need to go—to the point where we stabilize the network, reduce the incidents and their severity down to a minimum, and where they are no longer visible to the campus."

Dick Jacobson, North Dakota State University System IT security officer, attributed

his institution's success in part to organizational changes. "I think our program is effective, and the effectiveness has grown because of the formalized structure that we have put in place with designated security officers on the campuses. There is a defined flow of communication."

Morrow Long, information security director at Yale University, measured success by incrementally improving IT security programs. "IT security at Yale University is effective: over time we have been able to achieve quite a bit in terms of increasing security—moving the university off insecure protocols and implementing internal firewalls, authentication systems, standards, policies, and procedures for securing machines. It is an incremental, evolutionary approach, year by year—but we have moved quite a bit in terms of where we were."

Paul Howell, information systems security officer at the University of Michigan, is more cautious about success. "It is hard to judge

success because we are really in the business of risk management. If nothing happens, does that mean we are successful? Or if there is a major, national-headline incident, does that mean we are unsuccessful?"

The absence of benchmarks—a problem for higher education in all business areas—makes it difficult to measure success.

IT Security: What Matters

Our data show that although using more sophisticated technologies has significantly enhanced IT security, institutions have placed even more importance on the human and cultural factors of campus life. They recognize that they must address “human frailty” for the higher education environment to be secure. Indeed, our data show that respondents perceive managing security to be at least as much of a people problem as a technology problem. In the following sections, we demonstrate that “soft” IT security interventions (organization, policies, awareness programs, executive attention) seem

to make respondents feel more secure than do “hard” interventions such as technology investments.

Organization Matters

Table 8-2 compares opinions about success among institutions that have a dedicated IT security staff, a single staff member, and a distributed staff. It shows that institutions with a dedicated staff do markedly better in all five areas. We attribute this to the activities that dedicated security staff can and have undertaken and completed. A dedicated staff has the time to see that various IT security tasks are done, and in a more holistic manner. The presence of a dedicated staff (more prevalent at larger institutions) can denote a level of professionalism, which then drives practices and procedures implemented and technology deployed. The number of staff employed was less significant than having a dedicated staff. The staff’s experience also seemed to make a difference: institutions with staff who had more than three years

Table 8-2. Success of IT Security, by Staffing Pattern

Staffing Model		Program Is Successful	Beyond Requirements	Systems Are Secure	Metrics Developed	More Secure than Two Years Ago
Single staff member	Mean	2.47	3.34	2.78	3.57	1.94
Dedicated security operations staff	Mean	2.00	2.98	2.49	3.06	1.56
Spread across multiple functions	Mean	2.28	3.31	2.67	3.59	1.89

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

of experience felt they were doing better than those whose staff had three years or less of experience.

IT Security Policies, Planning, and Formal Risk Assessments Matter

In Chapter 5 we noted the adoption level of formal IT security policies and presented some of the reasons for putting policies in place. Our data (see Table 8-3) show that institutions with IT security policies in place characterize their IT security programs

as more successful and feel more secure today. Michael McRobbie, vice president for information technology and CIO at Indiana University, advised, “Policy comes first; then security. You can get preoccupied with tactics and lose sight of the grand scheme. You need constant policy education. Put policies in place that make security possible.”

We also find an improved sense of security when IT security is part of an IT security plan (see Table 8-4). Note also that metrics are more likely to have been developed at

Table 8-3. Success and Formal Institutional Policies

Formal Institutional Policies		Program Is Successful	More Secure than Two Years Ago
Yes	Mean	2.110	1.760
	Std. deviation	0.684	0.792
No	Mean	2.550	1.990
	Std. deviation	0.777	0.864
Total	Mean	2.310	1.860
	Std. deviation	0.759	0.833

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Table 8-4. IT Plan Characteristics and Perceived Success

Security Part of IT Plan		Program Is Successful	Metrics Developed	More Secure than Two Years Ago
Yes	Mean	2.200	3.370	1.760
	Std. Deviation	0.753	0.892	0.796
No	Mean	2.540	3.870	2.180
	Std. Deviation	0.670	0.755	0.893

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

institutions that have an IT security plan and audit regularly.

Also, we find a similar improved sense of security when risk assessments have been completed (see Table 8-5).

Leadership Matters

We asked respondents whether their president and provost had been active in developing IT security policy (see Table 8-6). While the mean is lower than expected overall, we clearly see an impact when the

president and provost are involved. At institutions where the president is involved, for example, the mean score for success is 3.18, compared with 4.50 at institutions where the president has not been involved (measured on a 5-point Likert scale, with 1 being highly successful and 5 being highly unsuccessful).

Clark Sorensen, manager of information systems and services and senior assistant registrar at Indiana University, emphasized the importance of leadership. “Since McRobbie came on campus, the campus

Table 8-5. Success and Risk Assessment Undertaken

Risk Assessment Undertaken		Program Is Successful	Metrics Developed	More Secure than Two Years Ago
Yes	Mean	2.03	3.15	1.64
	Std. Deviation	0.745	0.892	0.684
No	Mean	2.44	3.71	1.97
	Std. Deviation	0.742	0.829	0.851

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Table 8-6. Impact of the President and Provost in Developing Policy

Program Success	President Involved	Provost Involved
Highly successful	3.18	3.28
Fairly successful	3.64	3.35
Neither	3.86	3.69
Fairly unsuccessful	3.92	4.00
Highly unsuccessful	4.50	4.50
Total	3.67	3.47

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

culture regarding security has changed. We more stringently ensure that people don't get to data that they shouldn't have. People at Indiana University are taking IT security seriously."

McRobbie advised, "Get your president on your side. Get him to say security is important publicly." McRobbie immediately established a good working relationship with then-President Myles Brand, who became a strong advocate for IT security. Executive-level support enabled Indiana University to proceed more quickly in adopting good security practices than it could have without this support.

Size Matters

We looked at the size of institutions along three dimensions: enrolled students, number of devices on the network, and number of users on the network. We then tested to

see if size mattered, and if so, where. As we demonstrate, size does matter. And most often, it is the number of devices on the network that seems to matter most.

Table 8-7 shows that as the number of network devices increases, the likelihood of having a dedicated IT security staff increases. As institutions grow to more than 5,000 devices, they begin to deploy a dedicated IT security staff. And as we noted earlier in this chapter, the presence of a dedicated IT security staff has a noticeable impact on IT security and behavior at institutions.

Similarly, we found a greater likelihood of having a formal policy (Figure 8-1) and a formal incident handling procedure among institutions with more than 5,000 networked devices.

As the number of devices increases, the issue of decentralization causes greater concern (Figure 8-2), as does the fear of an

Table 8-7. Number of Devices and Staffing Patterns

Number of Devices	Staffing Pattern (Percentage of Respondents)			
	Single Staff Member	Dedicated IT Security Staff	Decentralized Security Staffing	Other
Under 1,000	29.4	0.0	50.0	20.6
1,001–5,000	26.4	2.6	59.6	11.4
5,001–10,000	24.3	18.9	51.4	5.4
10,001–20,000	4.3	27.7	66.0	2.0
20,001–40,000	0.0	30.4	65.2	4.4
40,001–60,000	8.3	41.7	50.0	0.0
More than 60,000	0.0	55.0	45.0	0.0

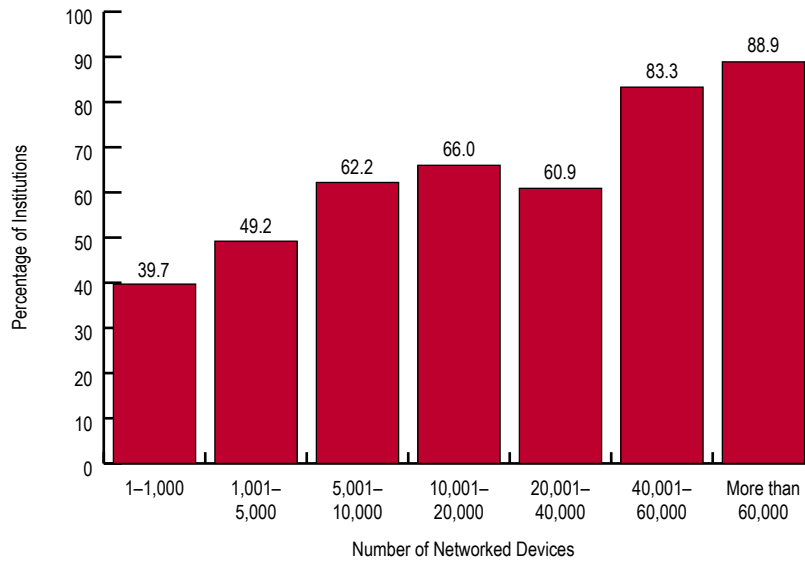


Figure 8-1.
Relationship
Between IT
Security Policies
and Networked
Devices

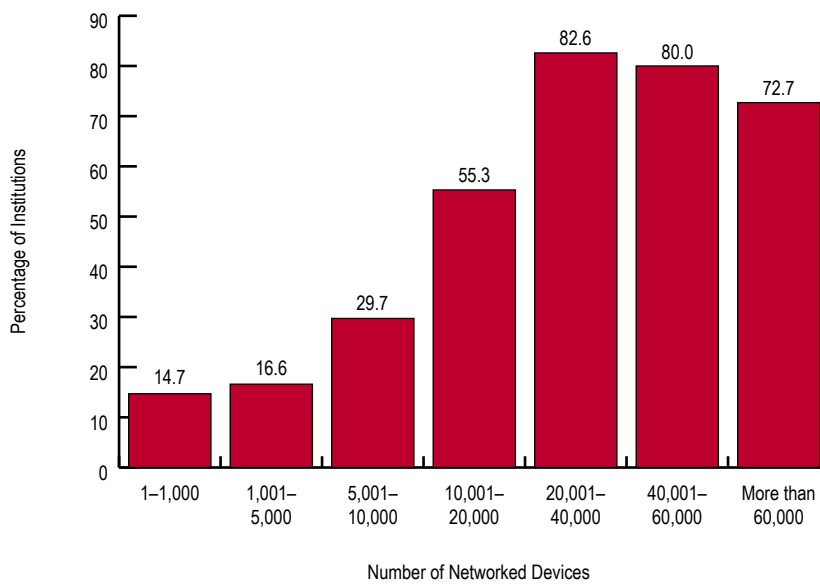


Figure 8-2.
Decentralization
Perceived as IT
Security Barrier,
by Number of
Networked
Devices

IT security problem occurring because of an authorized campus user's inadvertent action (Table 8-8).

Awareness Programs Matter

Similarly, the presence of awareness programs increases the sense of security (see Table 8-9). Awareness programs and IT security go hand-in-hand.

Money Matters

Absence of resources was by far the largest barrier to IT security for our respondents. We asked five questions about the IT security budget: What percentage of the IT budget is spent on security? Does the institution provide sufficient funds for IT security?

(The latter question used a 5-point Likert scale, with 1 being strongly agree and 5 being strongly disagree.) How does budget impact IT security? Do you feel better? Are purchases of technology affected?

Table 8-10 indicates the percentage of the central IT budget spent on security and compares respondents' mean assessments of IT security program success and whether they feel more secure today than two years ago. It appears that the more you spend, the better you feel!

Similarly, respondents who believe their institution provides necessary resources give higher ratings for IT security program success and their current sense of IT security (Table 8-11). The data also show that institutions

Table 8-8. Concern for Problems Caused by Authorized Users, by Number of Networked Devices

Number of Devices	Mean	Std. Deviation
Under 1,000	2.88	0.937
1,001–5,000	2.71	1.105
5,001–10,000	2.51	1.010
10,001–20,000	2.34	0.891
20,001–40,000	2.17	0.834
40,001–60,000	2.33	0.651
More than 60,000	1.60	0.548

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Table 8-9. Success and Awareness Programs for Staff

Formal IT Security Awareness Program for Staff		Program Is Successful	More Secure than Two Years Ago
Yes	Mean	2.000	1.660
	Std. deviation	0.592	0.661
No	Mean	2.500	1.980
	Std. deviation	0.799	0.898

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Table 8-10. Assessment of IT Security Program Success Compared with IT Budget

Percentage of Central IT Budget for IT Security	Program Is Successful	More Secure than Two Years Ago
Less than 1	2.56	2.16
1–5	2.30	1.82
6–10	2.00	1.62
11–15	1.60	1.20
16–20	1.50	2.00
Over 20	1.00	1.00

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Table 8-11. IT Security Program Success Compared with Resources Provided

Institution Has Provided Needed Resources	Program Is Successful	More Secure than Two Years Ago
Strongly agree	1.30	1.20
Agree	1.92	1.65
Neutral	2.28	1.81
Disagree	2.50	1.97
Strongly disagree	2.96	2.28
Total	2.31	1.86

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

that spend a higher percentage of the IT budget on security and provide sufficient resources have purchased more technology and invested more in awareness programs. Money matters!

IT Security Barriers

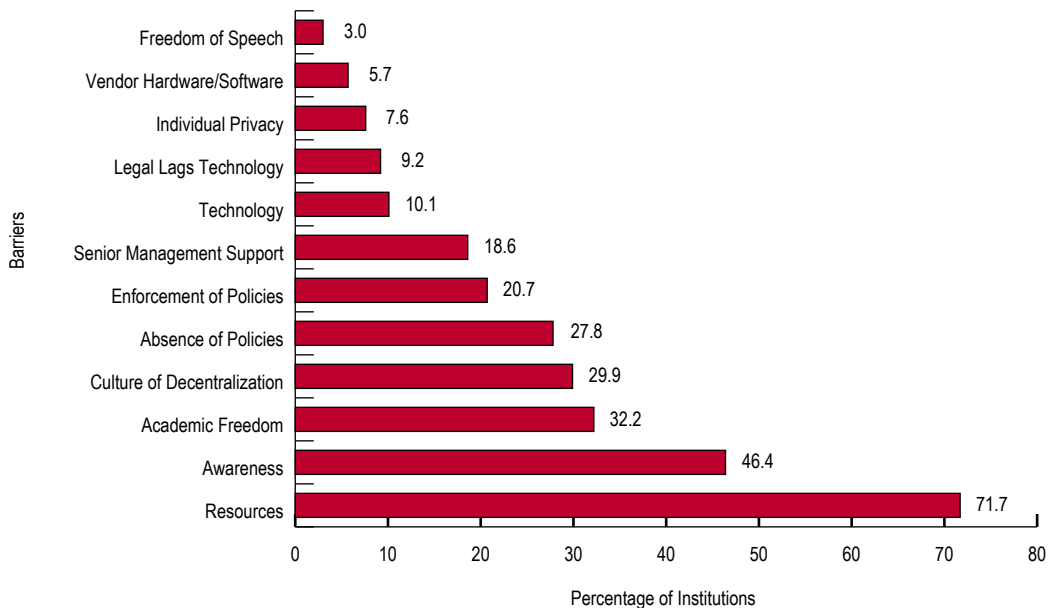
We have discussed at some length factors that contribute to IT security programs' success. We turn now to barriers that hinder IT security.

We asked respondents to identify and assess barriers to IT security at their institutions (see Figure 8-3). By far the most common problem cited was lack of resources (72 percent), followed by lack of awareness (46 percent) and cultural reasons such as academic freedom (32 percent) and culture of decentralization. External factors such as laws and their timely implementation and clarification, technology, software, and hardware scored much lower. We were surprised by the lower scores given to vendor hardware and software and the legal environment.

We looked at Carnegie class to find any major differences of opinion by institution type and found little, with two exceptions. Not surprisingly, a culture of decentralization was primarily an issue at doctoral institutions. Baccalaureate institutions most often mentioned individual privacy, but the percentage was low in any event. President James Wright of Dartmouth College believes the complex interrelationship between security and privacy will emerge as the most controversial issue.¹

Respondents saw decentralization as a barrier at many complex institutions. At Indiana University, for example, respondents noted the natural tension and synergy between the centralized policy development and security programs and the decentralized units. According to Beth Cate, associate university counsel, "Tensions can arise because some units historically have operated their systems in a decentralized way and generally favor as much autonomy as possible in the services of academic freedom, but their technological expertise and resources may vary

Figure 8-3.
Perceived
Barriers to IT
Security



and create substantial risks to the security of those systems. The key in lessening this tension is good communication between the centralized IT offices and the units that emphasizes the help that the central offices can provide the units in meeting their computing needs while ensuring an appropriate level of security for their systems, and that also educates the units about the risks involved with decentralization.”

Paul Howell, information systems security officer at the University of Michigan, provided a fairly typical assessment of institutional barriers. “Money and resources are always issues,” he said. “We have a lot of legacy equipment. The decentralized nature of the university from a security viewpoint is more of a hindrance than help. Sponsored research needs to be operated in a secure manner and is expected to do so by the federal government. But it does not appear that the federal government wants to provide funding for this purpose. We need a greater partnership between universities and the federal government and a reexamination of the infrastructure or overhead that exists around hosting research work.” Competent system administration time, security technologies, and training costs escape the research and research funding processes.

Bruce Judd, associate vice president at San Jose State University, commented on the legal environment. “There are new laws in California that require institutions to notify affected individuals if their systems get hacked and they lose information of a personal and individual nature. Individuals now have legal remedies available that would put the university in a legally liable situation. Security now is mission critical in terms of keeping our heads above water legally.” Mike Adelaine, CIO at South Dakota State University, noted further: “Land grant institutions have to interface with all of the usual campus constituencies, the general

public, and many state and federal government agencies. State government particularly has much stricter security policies in place. We need to lower our guard to let our faculty and students conduct their business, but the state government absolutely will not make exceptions. It will be hard to maintain high IT security and open access that is acceptable to both sides.”

The upshot of the legal environment is that tighter technical controls on university systems seem inevitable. “It is likely that our systems are going to be less open to nefarious activities than previously,” predicted Eric Cosens, information systems auditor at Indiana University. “We want to be as open as we can for our educational mission, but higher education is tricky—a balancing act. It’s like walking a tightrope. I’d like to see more intelligent control technologies developed and exploited. Allowing for freedom while having adequate controls in place is the goal.”

Our respondents concurred. A majority (57 percent) agreed that centralized networks and network management were the only way to be able to comply with federal and state requirements concerning IT security. Only 15 percent disagreed or strongly disagreed. Likewise, a majority (66 percent) agreed that standardized networks and network management were necessary to comply with federal and state requirements concerning IT security. Only 9 percent disagreed or strongly disagreed.

Philip Long, CIO at Yale University, provided an interesting perspective on technology as a barrier. “One barrier that is just gigantic is the software that vendors deliver to us, especially in an enterprise situation. We constantly get vendor products that say they have good security. They imagine that we can create a password and net ID for their particular use and somehow their product will exist on a campus as if it were a

stand-alone item.” Jeffrey Schiller, network manager at the Massachusetts Institute of Technology, also noted this issue. “Packaged systems are difficult for us to integrate because they tend to rely on firewalls and VPNs to provide security [rather than incorporating security into the product]. If a vendor says you need a firewall, that’s a warning sign.”

We found no significant differences on the opinions above by Carnegie class or country.

Impact of Perceived Barriers on Success

Are perceptions of barriers and success linked? In some cases, yes, but in most cases, no. Respondents who thought institutional security policies posed no barrier to success at their institution rated IT security success and their sense of security higher. We found similar relationships for technology and senior management support.

Melding IT Security with Internal Business Practices

A majority (55 percent) of respondents indicated that business requirements take precedence over IT security when the two conflict. Only 17 percent of respondents disagreed or strongly disagreed. This confirms the anecdotal belief that functionality takes precedence over IT security in higher education when new systems are installed. However, respondents who believed security took precedence at their institutions were twice as likely to indicate that their security

programs were a success and that they felt more secure than two years ago.

Similarly, most respondents (75 percent) agreed that their institution’s IT architecture and implementation sacrificed some level of protection to ensure ease of use. Only 9 percent disagreed or strongly disagreed.

Some institutions appear to have found an acceptable balance by interweaving IT security with their business practices. Terri Wiskirchen, university risk manager at Embry-Riddle Aeronautical University, noted, “Whenever we look at new systems, new software, or new processes, security is an integral part of the consideration.” At Yale University, Morrow Long believes IT security is woven pretty well into the fabric of business. “In 1997 we built IT security into the new administrative system and into training—how to get accounts, access, and roles and responsibilities,” he said. “HIPAA [the Health Insurance Portability and Accountability Act] forced the medical school to increase information security awareness as well. In research, security is probably not woven as well. Researchers tend to be closed off in their own little worlds. The medical school has done good outreach to the medical researchers to let them know that if they are dealing with clinical or any other personally recognized health information, they have to follow certain privacy standards.”

Endnote

1. D. Ward and B. L. Hawkins, “Presidential Leadership for Information Technology,” *EDUCAUSE Review*, Vol. 38, No. 3, May/June 2003, p. 45.