

7

IT Security Program Success: What Matters

We never know, believe me, when we have succeeded best.

—Miguel de Unamuno

Key Findings

- ◆ Respondents feel more secure today than they did two years ago despite being in a perceived riskier environment. This is particularly true of institutions with IT security plans in place.
- ◆ The respondents who believe their institution provides necessary resources rate their IT security program's success higher and feel more secure than others.
- ◆ The biggest barrier to IT security is lack of resources, especially at smaller institutions, followed by an academic culture of openness and autonomy, and lack of awareness.
- ◆ Respondents feel the academic community has become more sensitive to security and privacy in the last two years.

Successful IT security depends heavily on the presence of IT security plans, risk assessments, audits, awareness programs, the IT security culture, and budget. In this chapter we make comparisons between 2003 and 2005 to determine what has and has not changed. We point especially to conclusions and recommendations of the CIFAC study, which has identified important trends and best practices, and has articulated numerous recommendations for improving IT security on our campuses (Rezmierski, Rothschild, Kazanis, & Rivas, 2005).

How Successful Are We?

We used a Likert scale ranging from 1 to 5 (1 = strongly disagree, 2 = disagree, 3 = neutral,

4 = agree, and 5 = strongly agree) 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 six questions:

- ◆ How would you characterize your program's success?
- ◆ Has your institution gone beyond federal and state government IT security requirements?
- ◆ Are central data, networks, and applications that are your responsibility secure?
- ◆ Are locally controlled data, networks, and applications secure?
- ◆ Have you developed metrics to determine IT security activities' effectiveness?
- ◆ Is your institution more secure today than it was two years ago?

©2006 EDUCAUSE. Reproduction by permission only.

We calculated the mean for each question and then compared the means by Carnegie class, along with a category for Canadian institutions (see Table 7-1). The respondents were most positive about feeling more secure today than two years ago despite being in what we perceive to be a riskier environment. The means, which are all over 4.00, show that a majority agreed or strongly agreed that their institutions are more secure today. The next most positive response was to the question on the security of central IT assets. Overall,

Canadian respondents scored their security higher than their U.S. counterparts.

For the most part, assessing security level remains, for many institutions in our survey, a subjective exercise.

We then compared the answers of respondents who participated in both the 2003 and 2005 surveys to see what changes had taken place, if any (Table 7-2). What we found was a lower assessment of the success of the IT security program, even though respondents felt slightly more secure

Table 7-1. Assessment of Campus Security Outcomes (N = 466)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics	More secure today
DR	3.58	3.16	3.81	2.87	2.82	4.38
MA	3.24	2.91	3.83	3.08	2.46	4.14
BA	3.25	2.88	3.84	3.42	2.43	4.00
AA	3.60	2.88	3.92	3.85	2.59	4.16
Canada	3.66	4.27	4.18	3.73	2.70	4.48

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Table 7-2. Assessment of Campus Security Outcomes, 2003 and 2005 (N = 204)

	The IT security program at my institution is successful.		The centrally controlled data, networks, and applications are secure.		I feel my institution is more secure today than it was two years ago.	
	Mean 2005	Mean 2003	Mean 2005	Mean 2003	Mean 2005	Mean 2003
DR	3.62	3.77	3.83	3.24	4.33	4.20
MA	3.35	3.55	3.91	3.14	4.23	3.95
BA	3.11	3.74	3.89	3.53	3.89	4.14
AA	3.88	3.84	4.11	3.63	4.37	4.28
Canada	3.45	3.73	4.09	3.36	4.18	4.09

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

in 2005 than in 2003. This may be due to a heightened awareness of the complexity of the threats and the multidimensionality of an IT security program. Respondents offered a significantly higher assessment of central security networks and data.

We also looked at whether respondents had gone beyond federal and state regulations and developed better metrics in two years. We found that they had paid more attention to regulations, but metrics changed little (see Table 7-3). Baccalaureate institutions showed a decline in both categories. Canadian institutions showed the largest increase in mean response to these questions.

IT Security: What Matters

Our data show that although using more sophisticated technologies has 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 (plans, risk assessments, audits, and awareness programs) seem to make respondents feel more secure than do “hard” interventions such as technology investments.

In 2003, we found that institutions had primarily focused their efforts in the technology arena. In 2005, we found a more balanced approach, with both technical and cultural solutions employed at many institutions, although for many of the soft approaches, there is still significant room for improvement.

IT Planning, Formal Risk Assessments, and Security Audits Matter

In Chapter 5, we noted the adoption level of formal IT security plans. Our data (see Table 7-4) show that respondents from institutions with IT security plans in place characterize their IT security programs as more successful and feel more secure today. The differences are dramatic. Institutions with an IT plan in place have a mean of 4.02 in terms of perception of success, versus 3.08 for those with no plan. Planning also increases responsiveness to government regulation and metrics. Planning apparently has less of an impact on IT security for locally controlled networks and data. We

Table 7-3. Regulations and Metrics in 2003 and 2005 (N = 204)

	Went beyond regulatory recommendations for IT security		Developed metrics to determine IT security effectiveness	
	Mean 2005	Mean 2003	Mean 2005	Mean 2003
DR	3.09	2.81	2.67	2.63
MA	2.69	2.48	2.22	2.16
BA	2.69	2.82	2.19	2.50
AA	3.26	3.00	2.63	2.68
Canada	3.50	2.80	2.55	2.27

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Table 7-4. Perceived Impact of IT Security Plan (N = 490)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics	More secure today
Comprehensive plan in place	4.02	3.67	4.15	3.18	3.18	4.56
Partial plan in place (or some units have plan)	3.45	3.05	3.85	3.21	2.61	4.22
Neither a comprehensive nor partial plan in place	3.08	2.76	3.77	3.45	2.10	4.00

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

note that the CIFAC study considers having and following written policies and procedures to be one of the most important factors in preventing incidents, second only to education, training, and awareness (Rezmierski, Rothschild, Kazanis, & Rivas, 2005).

Also, with the exception of locally controlled networks and data auditing, we find a similar improved sense of security when risk assessments and security audits have been completed (see Tables 7-5 and 7-6).

Awareness Programs Matter

The 2005 Cybersecurity Summit stressed the importance of user awareness and education: "Consistent with most areas of cybersecurity, the effort to keep owners and users of data aware of the threats, and methods to mitigate the threats, must be maintained and increased. Communication between major data centers to discuss, develop and update best practices should be encouraged. They recommended that centers should publish minimum user best practices for data security and integrity, and encourage adherence to best practices" (Rezmierski, Rothschild, Kazanis, & Rivas, 2005, p. 21). The CIFAC study substantiates the importance of this

best practice: "The two most frequently recommended foundational basic best practice for mitigating the effects of an incident was straightforward communication with affected individuals; this was followed by the establishment and use of interdepartmental communication and collaboration to handle the problem" (p. 41). The CIFAC study further concludes that for 70 percent of IT managers, education and training were important for preventing security incidents.

Institutions that have managed to instill IT security practices as an integral part of their culture score better than institutions that have not (see Table 7-7). But accomplishing this is no easy matter. According to Jack Suess of the University of Maryland, Baltimore County, "Higher education's challenge is that cultural change is very difficult. Cultural change is probably almost impossible if it is pushed solely from within the IT organization and without a broader institutional buy-in from the academic and senior leadership. Their support is the only way people will take seriously their individual role in improving campus IT security."

And then there is the nature of a university's business. Joy Hughes, CIO and vice president, information technology at George

Table 7-5. Risk Assessment Status and Perceived Success (N = 490)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics
No risk assessments done	3.22	2.85	3.80	3.29	2.29
For some institutional data and asset types	3.56	3.15	3.88	3.16	2.73
For all institutional data and asset types	3.76	3.45	4.24	3.67	3.10

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Table 7-6. IT Security Audits and Perceived Success (N = 489)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics	More secure today
Not performed	3.21	2.68	3.72	3.33	2.24	3.91
On an irregular basis	3.45	3.06	3.87	3.22	2.56	4.30
On a regular basis	3.57	3.38	3.99	3.25	2.95	4.34

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Mason University, observes, “As long as our university conducts research, we will be vulnerable. I can picture a teaching institution eventually becoming secure. It is harder at an institution with intensive research. The difficulty is not due to the faculty’s attitudes and their intentions. Rather, it is due to their research activities. For example, oceanic researchers conduct research using data from sensors that are located all over the world on the ocean floor, on boats, and on satellites.

How do you secure that network? The challenges are formidable.”

The presence of awareness programs increases the sense of security (see Table 7-8). Awareness programs and IT security go hand-in-hand, and the programs do affect the institutional culture.

Money Matters

A lack of resources was by far the largest barrier to IT security for our respondents. We

Table 7-7. Culture and Overall IT Security (N = 488)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics	More secure today
Strongly disagree	2.81	2.54	3.65	2.76	2.16	4.14
Disagree	3.12	2.83	3.74	3.16	2.26	4.15
Neutral	3.54	3.11	3.91	3.44	2.61	4.09
Agree	3.90	3.38	4.06	3.34	3.04	4.40
Strongly agree	3.94	3.69	4.07	3.31	3.25	4.75

Q: IT security is now a part of our institutional employee culture.

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Table 7-8. Institution Communicates Awareness and Overall IT Security Issues (N = 488)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics	More secure today
Strongly disagree	3.05	2.63	3.58	2.89	2.05	3.89
Disagree	3.08	2.72	3.77	3.34	2.22	3.94
Neutral	3.43	3.02	3.87	3.25	2.52	4.26
Agree	3.59	3.21	3.87	3.23	2.79	4.26
Strongly agree	3.85	3.36	4.12	3.36	2.79	4.67

Q: My institution communicates IT security awareness issues to its faculty, students, and staff regularly.

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

asked two questions about the IT security budget. Does the institution provide sufficient funds for IT security? What percentage of the IT budget is spent on security? We asked for each respondent’s opinion on the success of

his or her institution’s IT security programs and on benchmarks for success that were related to funding (see Tables 7-9 and 7-10).

Respondents who believe their institution provides necessary resources give higher rat-

Table 7-9. Adequate Funding and IT Security (N = 490)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	Developed metrics	More secure today
Strongly disagree	2.55	2.19	3.67	2.84	1.98	3.90
Disagree	3.22	2.74	3.81	3.22	2.35	4.18
Neutral	3.44	3.08	3.77	3.40	2.61	4.12
Agree	3.84	3.53	3.99	3.32	2.89	4.37
Strongly agree	4.21	3.89	4.47	3.37	2.89	4.74

Q: My institution has provided the needed resources to address the institution’s IT security issues.

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Table 7-10. Expenditures and Overall IT Security (N = 490)

	Program success	Beyond government recommendations	Secure central systems and data	Secure locally controlled data, networks, and applications	More secure today
Less than 1%	3.00	2.47	3.77	3.26	3.95
1–5%	3.46	3.00	3.85	3.13	4.21
6–10%	3.58	3.30	3.99	3.49	4.30
11–15%	3.67	3.67	4.45	3.92	4.58
16–20%	3.75	3.75	3.75	3.00	4.63
Over 20%	3.33	3.00	4.33	4.00	4.67

Q: Percentage of the central IT budget dedicated to IT security.

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

ings for IT security program success and their current sense of IT security. The data also show that institutions 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!

Table 7-10 shows the percentage of the central IT budget spent on security and compares respondents’ assessments of IT security program success, indicating whether they feel more secure today than two years ago. It appears that the more you spend, the better you feel!

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 (see Table 7-11).

We asked respondents to identify and assess barriers to IT security at their institutions. By far the most common problem cited was lack of resources (64.4 percent), especially at smaller institutions, followed by an academic culture of openness and autonomy (49.6 percent) and lack of awareness (36.4 percent). Technology and privacy issues scored lowest.

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. Note that almost all of the barriers were related to people and their behavior and practices.

Table 7-12 indicates a perception of positive change from 2003 to 2005. Our respondents in general perceive that barriers have

been lessened, particularly cultural issues such as awareness and decentralization. In our 2003 study, we predicted that the severity of attacks on computers and networks would change community attitudes toward central management, and that prediction has come true. Particularly noteworthy is the rate of change on enforcement (34.3 percent), lack of awareness (29.1 percent), and senior management support (23.3 percent).

Melding IT Security and the Institution's Culture

The good news in Table 7-13 is that respondents feel the community has become more sensitive to security and privacy in the last two years (mean of 3.78). However, a majority of respondents agree or strongly agree (mean of 3.30) that business requirements take precedence over IT security when the two conflict. This confirms the anecdotal belief that functionality takes precedence over IT security in higher education. Indeed, most respondents (mean of 3.57) agreed that their institution's IT architecture and implementation sacrificed some level of protection to ensure ease of use. However,

Table 7-11. Barriers to Success (N = 492)

Barrier	Percentage
Lack of resources	64.4%
Academic culture that values openness and autonomy	49.6%
Lack of awareness	36.4%
Increased sophistication of threats	31.3%
Absence of policies	27.0%
Culture of decentralization	25.2%
Lack of senior management support	16.5%
Lack of enforcement of policies	14.6%
Technology issues	6.7%
Privacy of the individual	3.7%

Table 7-12. Perceived Changes to Barriers, 2003 to 2005 (N = 204)

Barrier	2005	2003	Institutional Change	Rate of Change
Lack of awareness	35.8%	50.5%	14.7%	29.1%
Culture of decentralization	29.9%	37.3%	7.4%	19.8%
Lack of enforcement of policies	13.2%	20.1%	6.9%	34.3%
Absence of policies	22.1%	27.0%	4.9%	18.1%
Lack of senior management support	13.2%	17.2%	4.0%	23.3%
Lack of resources	68.1%	71.6%	3.5%	4.9%
Technology issues	7.4%	8.8%	1.4%	15.9%
Privacy of the individual	4.4%	4.4%	0.0%	0.0%

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Table 7-13. The Institutional Culture (N = 492)

Issue	Mean	Std. Deviation
Individual behaviors have become more sensitive to security and privacy in the past two years.	3.78	0.770
IT security architecture and implementation sacrifices some level of protection to ensure ease of use.	3.57	0.858
Business requirements take precedence over IT security when there is a conflict.	3.30	0.931
IT security inhibits academic freedom.	2.37	1.011
IT security compromises personal privacy.	2.16	0.902
IT security unnecessarily limits user access to information.	2.01	0.776

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

respondents who believed security took precedence at their institutions were more likely to indicate that their security programs were successful and that they felt more secure than two years ago.

At the same time, issues such as academic freedom, privacy, and user access to information seem less problematic. Ced Bennett, emeritus director, information security services

at Stanford University, told us, "When I first started in my position at Stanford, the biggest hurdle was to get people to understand that openness, academic freedom, and security could coexist well. But there is a lot of myth out there to contradict that idea. The fact is that it should not be a question whether an individual can do something that they need to do or not, but rather, will it be more or

less convenient when they do it. Security sometimes requires some amount of inconvenience but shouldn't prevent anyone from accomplishing his or her objective. When you leave your home, the inconvenience is that you lock it with a deadbolt. When you ride your bike and leave it outside, the inconvenience is that you lock the bike or you don't own a bike anymore."

Respondents from the 204 institutions that participated in the 2003 and 2005 studies see a slight improvement in terms

of the assessment of business practices and ease of use (see Table 7-14).

Summary

We are struck by the notable changes that have occurred on the soft side of IT security. The higher education community has come a long way in the past two years in accepting prescribed behaviors to make their environment more secure. The culture has changed, and dramatically, but substantial room for improvement remains in many of these areas.

Table 7-14. Changes to Institutional Culture in Two Years (N = 204)

	Respondents	2005 Mean	2003 Mean	Rate of Change
Business requirements take precedence over IT security when there is a conflict.	204	3.27	3.41	-4.1%
My institution's IT security architecture and implementation sacrifices some level of protection to ensure ease of use.	204	3.60	3.83	-6.0%

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.