Higher Education Information Security Awareness Programs

ECAR

ECAR Research Bulletin | August 8, 2016

Joanna L. Grama, EDUCAUSE
Eden Dahlstrom, EDUCAUSE

Overview

In early 2016, the SANS Institute, an information security training and certification organization, released its second annual SANS Securing The Human report.[1] Based on a survey of 369 information security training and awareness professionals, the research is designed to understand the state of information security training and awareness programs across various industries, including "educational services."

The educational services industry represented 21% (n = 76) of the SANS survey responses, the largest sector represented in this research. SANS attributed the large response from the educational services industry to the fact that EDUCAUSE helped promote the survey among higher education information security awareness and training professionals.[2]

The 2016 SANS report shares the overall results of its research. However, due to large survey participation from the educational services sector, SANS graciously shared anonymized data results with the EDUCAUSE Center for Analysis and Research (ECAR) so that we could specifically report on the state of awareness and training programs in this sector. ECAR thanks EDUCAUSE members for their participation and SANS for its contribution of data to our understanding of higher education information security awareness and training programs.

Highlights

Awareness and education is an important part of any higher education information security program. Providing information security awareness training is a key factor in having a mature information security capability,[3] and ensuring that members of the institutional community (e.g., students, faculty, and staff) receive such awareness training is a critical information security capacity in higher education. In fact, in 2016, CIOs, CISOs, IT directors, managers, and staff all agreed that providing information security education and training was the top strategic information security issue.[4]

Given how critical such education can be to the institutional community, it is important to know how these programs are led and managed, how they are supported at the executive level, how mature they are, and the biggest challenges to their success. The key findings from this research cover four areas:

- **Leadership:** Information security awareness and training programs in higher education are typically led by managers who attend to training and awareness responsibilities with a fraction of an FTE.
- **Program Management:** Higher education information security awareness programs tend to be leanly staffed and have small budgets; programs are planned in an opportunistic manner.

- **Executive Support:** Higher education security awareness professionals generally feel that executives support institutional security awareness programs, but management is still often seen as the biggest obstacle to awareness program efforts.
- **Maturity and Metrics:** Higher education security awareness programs tend to be less mature than their counterparts in other industries, although a majority of institutions do track awareness program metrics for reporting purposes.

Leadership

Most of the respondents from the education sector reported that they had overall responsibility for their organizational security awareness program (see figure 1).

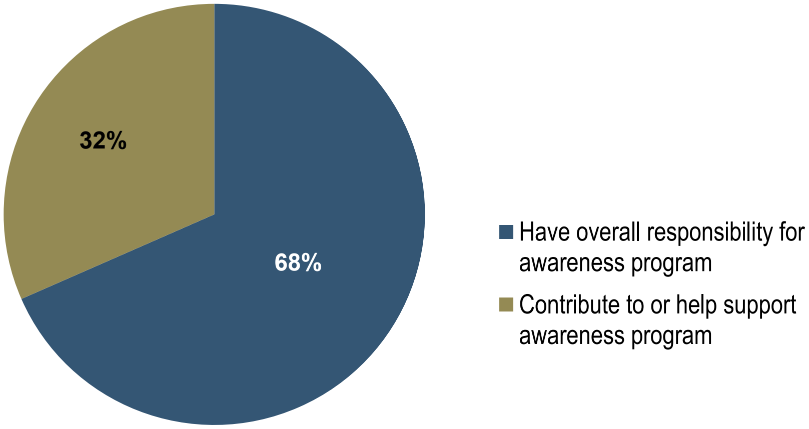

Figure 1. Respondent role in institutional security awareness programs (n = 76)

Among the educational services respondents to the SANS survey, a plurality were managers or directors (41%) at their institutions, while many others were individual contributors (37%). Only 22% indicated that they served at the executive level at their institution (defined as a senior director role or higher). The most common supervisor for security awareness professionals is the CIO or equivalent (39%). This structure is about twice as common as reporting to the CISO (20%) or an IT director/manager (21%). This is quite different from the other industry sectors represented in the SANS research, where the most common reporting line was to an IT director or manager (33%) or a CISO (32%). Only 13% of respondents outside the education sector said they report to a CIO[5] (see figure 2).

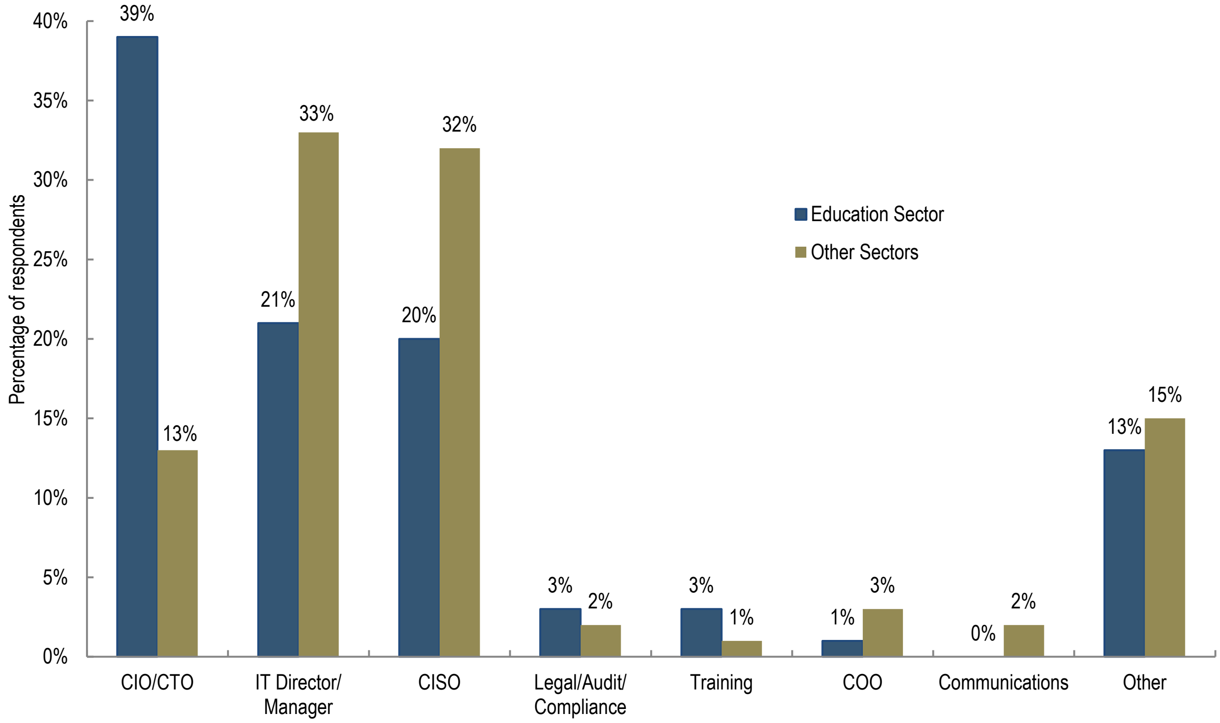

Figure 2. Respondent reporting line (education sector: n = 76; other sectors: n = 292) [6]

As in most industries, information security awareness and training in the educational sector is rarely a full-time job for a single individual. Instead, most individuals charged with information security awareness and training duties manage these activities as part of a larger set of job responsibilities. Only 5% of education sector respondents devote 90–100% of their time on such duties, which might indicate a full-time information security awareness and training role. Nearly 9 in 10 respondents (88%) reported that they spend up to half their time on information security awareness and training, indicating a part-time role at best. Most commonly, education sector respondents devote 15% or less of their time to awareness and training duties[7] (see figure 3).

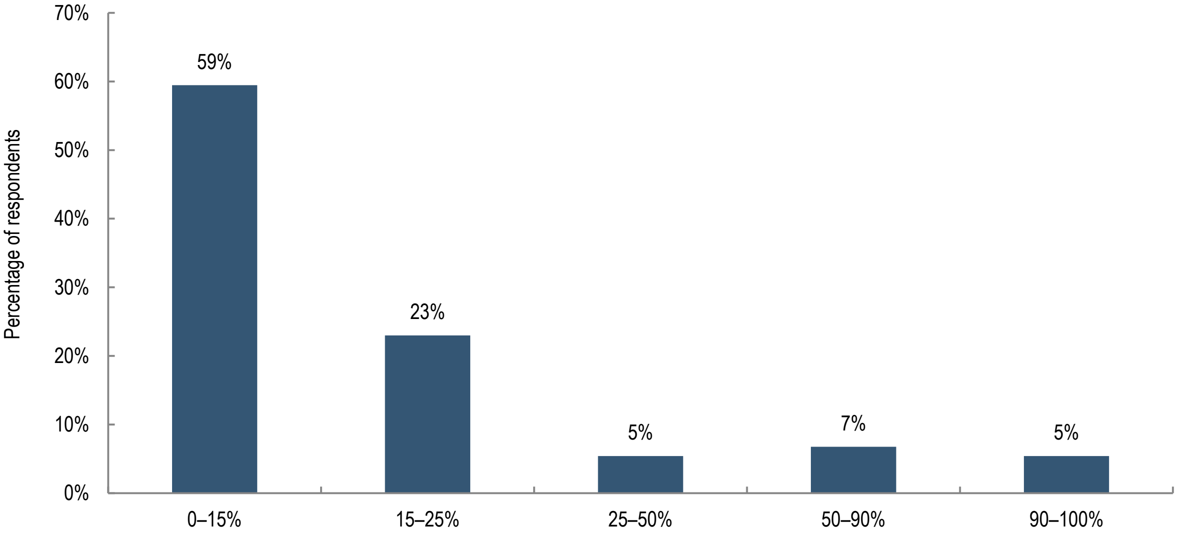

Figure 3. Percentage of time devoted to security awareness activities (n = 74)

Although a technical background is not a requirement to be successful as a security awareness practitioner,[8] the SANS educational services data show that most security awareness professionals have a background in information technology (58%) or physical or information security (26%). Only 11% of respondents came from communications, public relations, training, or other fields. This is neither statistically nor practically different from the SANS data set for noneducation industries, where 42% of respondents reported a prior role in information technology and 36% a prior role in physical or information security.[9]

Program Management

It is unlikely that all information security awareness professionals are introverts, but they do tend to work alone or on small teams that combine the efforts of more than one position to create a single full-time equivalent (FTE). Security awareness team size tends to be quite small, and team size is significantly and positively correlated with the number of people over whom the security awareness program has responsibility. That is, the more people a security awareness program is responsible for, the greater the FTE dedicated to security awareness. In the educational services sector, the size of the security awareness team is largely one FTE (23%) or less than one FTE (39%). Twenty-seven percent of institutions have teams of 2–3 FTE. Only 11% of the educational services respondents reported teams of four or more FTE. In higher education, where information security staff size is small in general (0.1 central IT information security FTE per 1,000 institutional FTEs[10]), it comes as no surprise that awareness teams are also small.

Awareness program 2016 budgets also tend to be small in the educational services sector. Budgets of less than $5,000 are most common, accounting for 53% of survey responses. About a quarter of survey respondents didn't know what their 2016 budgets would be; this was true for noneducation sector respondents to the SANS survey, too (see figure 4).

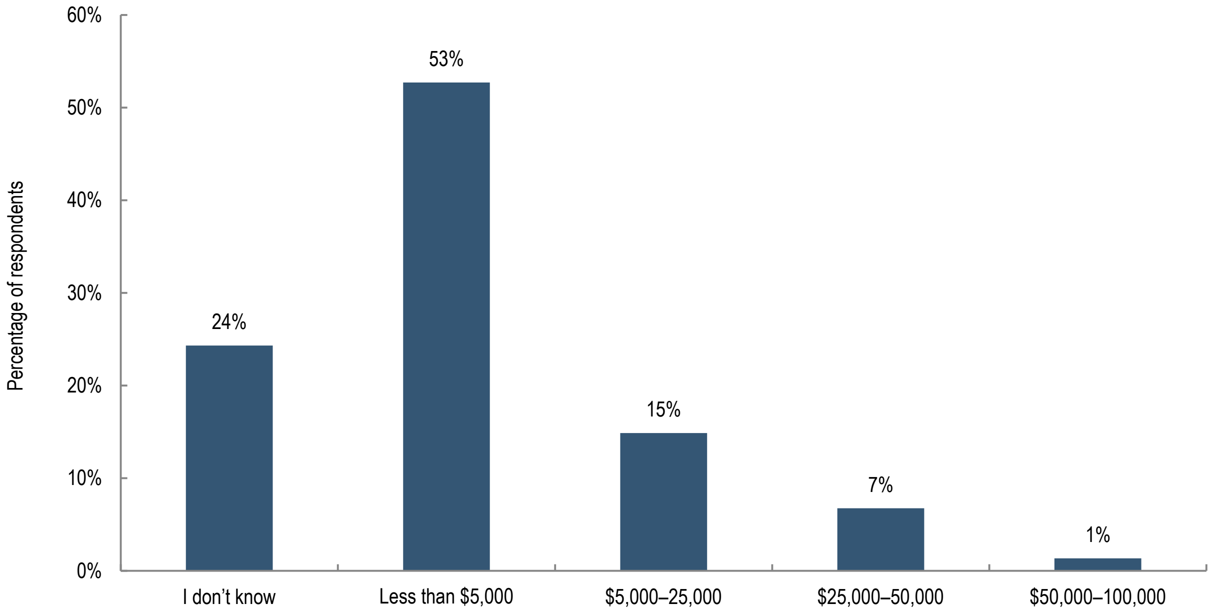

Figure 4. Estimated 2016 security awareness program budget (n = 74)

SANS asked respondents to share their approach to information security awareness activities in 2016. The responses in the educational services sector reflect the data noted above concerning the amounts of staff time and budgets that are devoted to awareness programs—relatively few people and dollars are dedicated to information security awareness. A majority of the respondents (55%) reported that awareness activities are conducted depending on the amount of time the responsible person has available. Only 11% of respondents reported a detailed awareness plan for 2016 that identifies audience targets and the topics that will reduce the most institutional risk. Figure 5 compares education and noneducation sector planning practices. The education sector reported a noticeably higher percentage of ad hoc/opportunistic planning practices than other sectors. In fact, education had the single highest percentage for this type of planning when compared to all other sectors (those with at least 10 respondents) individually in the SANS survey. Purposeful planning of awareness programs is an area for strategic growth in the education sector; however, it could be a challenge for the 62% of respondents who deliver security awareness programs with one or fewer FTEs dedicated to the work.

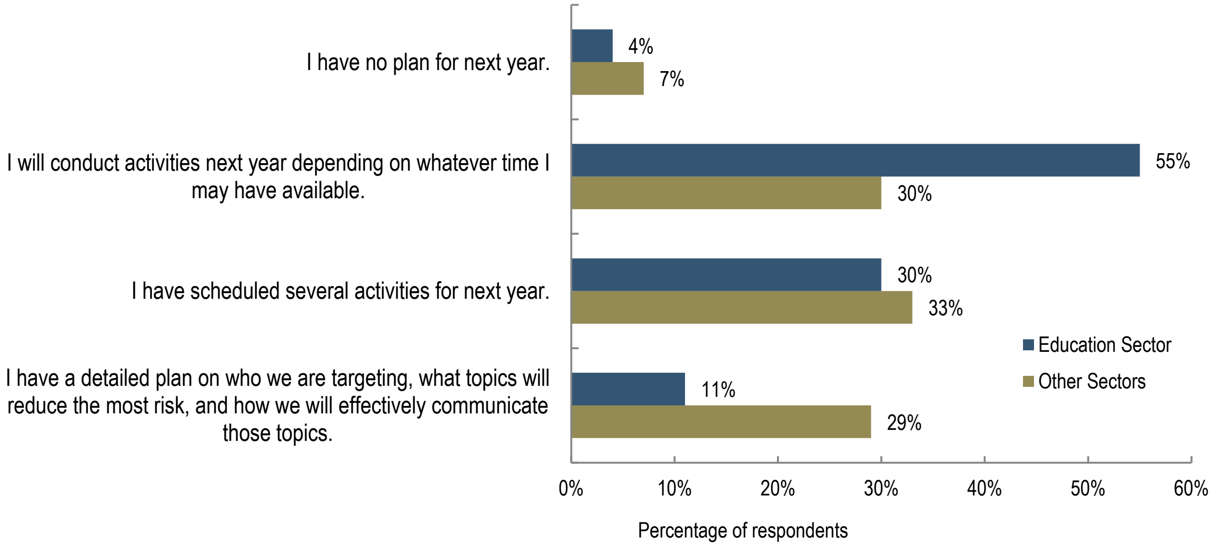

Figure 5. Organizations with 2016 security awareness program plans (education sector: n = 71; other sectors: n = 257)

Not surprisingly, resources (22%) and time (19%) were identified as two of the biggest challenges facing information security awareness programs in the educational sector (see figure 6). While culture as a stand-alone challenge was one of the top issues, it is important to note culture's critical role in change management. Peter Drucker is credited with the statement "culture eats strategy for breakfast," and culture can deflect or consume even the best strategic efforts. To overcome the biggest awareness program challenges, such as procuring more time or resources to support sound security practices, security awareness professionals will need to figure out how culture and strategy will be friends.

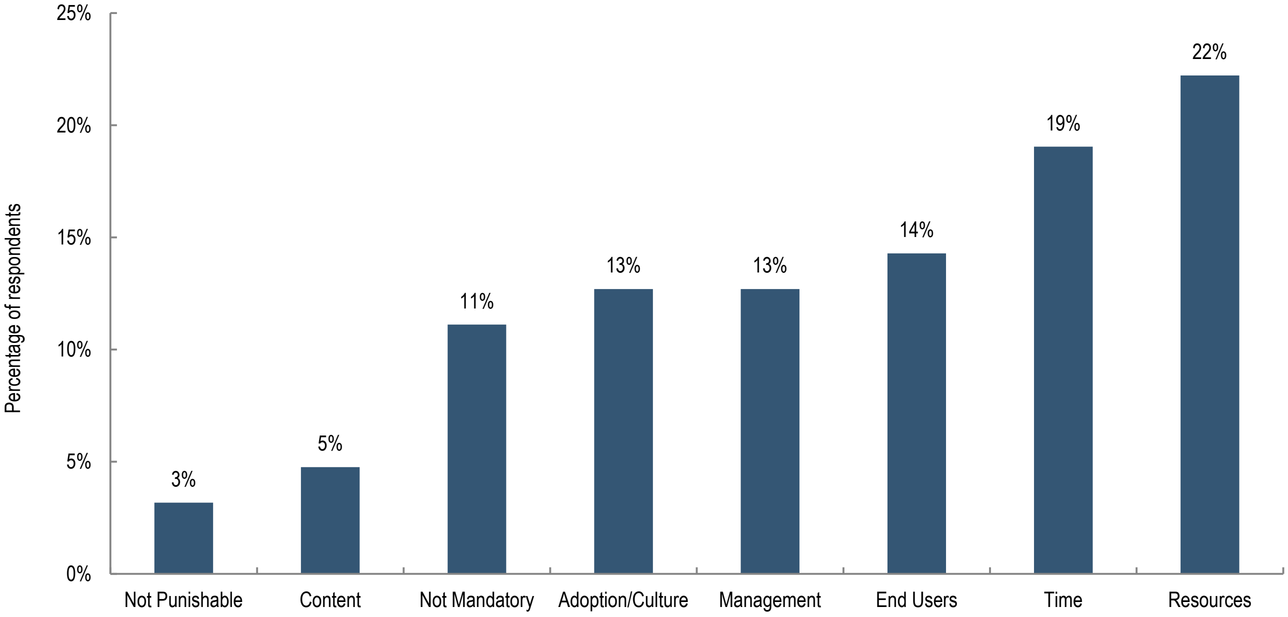

Figure 6. Security awareness program challenges (n = 63)

Although only 14% of survey respondents said that end users were their biggest security awareness challenge, effectively influencing end-user behavior is essential to managing security risks. To better understand organizational approaches that encourage appropriate secure-aware behavior, SANS asked survey respondents to share their institutional approach to information security compliance. The majority of responses (58%) from the educational services sector stated that the institution employs flexibility with respect to behavior correction. That is, security policies are "more like guidelines and should not get in the away of effectiveness."[11] This type of flexible response is no surprise in higher education, where teaching and learning, and not punishment, is a core value. In fact, no educational institution reported a punitive approach (see figure 7).

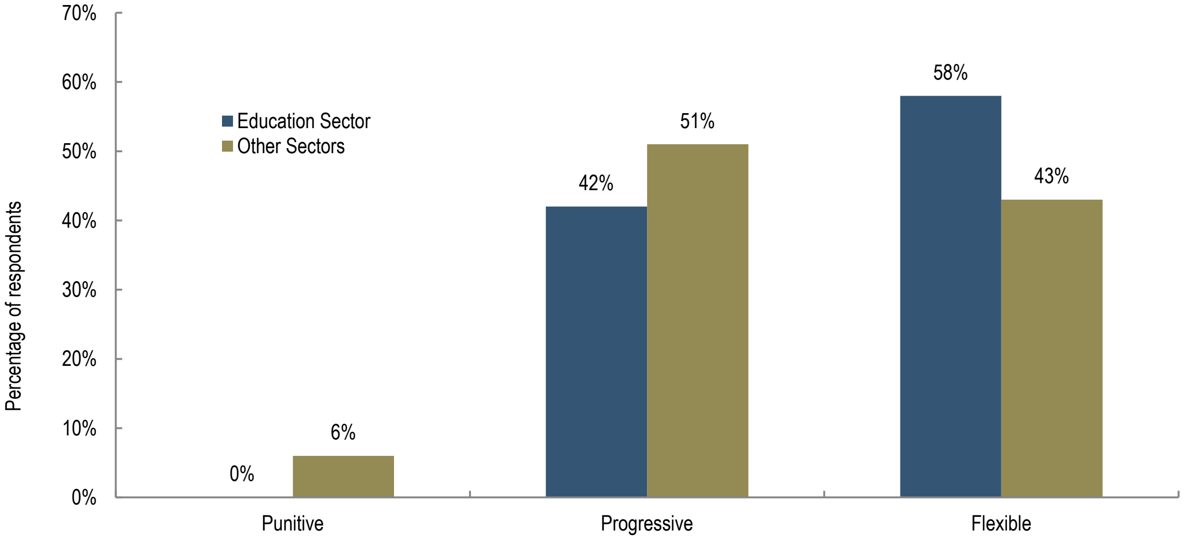

Figure 7. Security policy compliance approach (education sector: n = 69; other sectors: n = 256)

Executive Support

Executive support is critical for effective information security awareness programs. Awareness and training activities cannot become part of an institution's culture without the support of executive management. The SANS survey tried to understand how much management support information security awareness professionals believe they have for their program. In the educational services sector, a little more than half of the respondents felt that they have the executive support they need. Just under half reported less support than needed or no support. The balance between having and needing support suggests the importance of understanding individual institutional support needs. For security awareness program staff, this means assessing needs and communicating those needs through executive channels. For executives, this means actively asking what can be done to support unmet needs. On an interesting note, even though the option was available, no respondents in the educational services sector indicated that they had *more* executive support than needed (see figure 8).

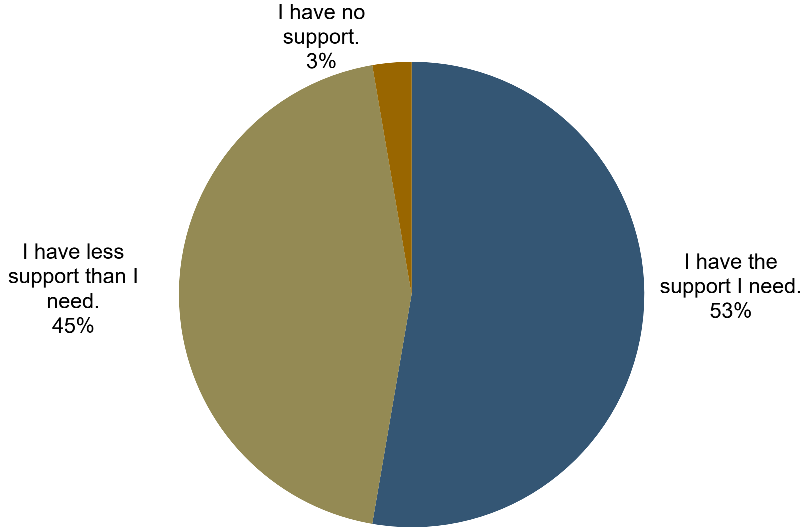

Figure 8. Executive support for security awareness programs (n = 74)

The SANS study also dug deeper into the notion of support by asking respondents which individual or role is the "biggest blocker" to information security awareness programs. Although 53% of respondents said they have enough executive level support, almost 15% of responses—which was the largest proportion—indicated that management is the biggest blocker of awareness programs, followed by end users (13%), and human resources (13%). Interestingly, 13% of respondents indicated that there were no blockers to organizational information security programs (see figure 9). At the other end of the scale, legal/audit was cited by only 3% of respondents as a blocker (serving as perhaps the only occasion that lawyers and auditors were not identified as obstacles to an initiative![12]).

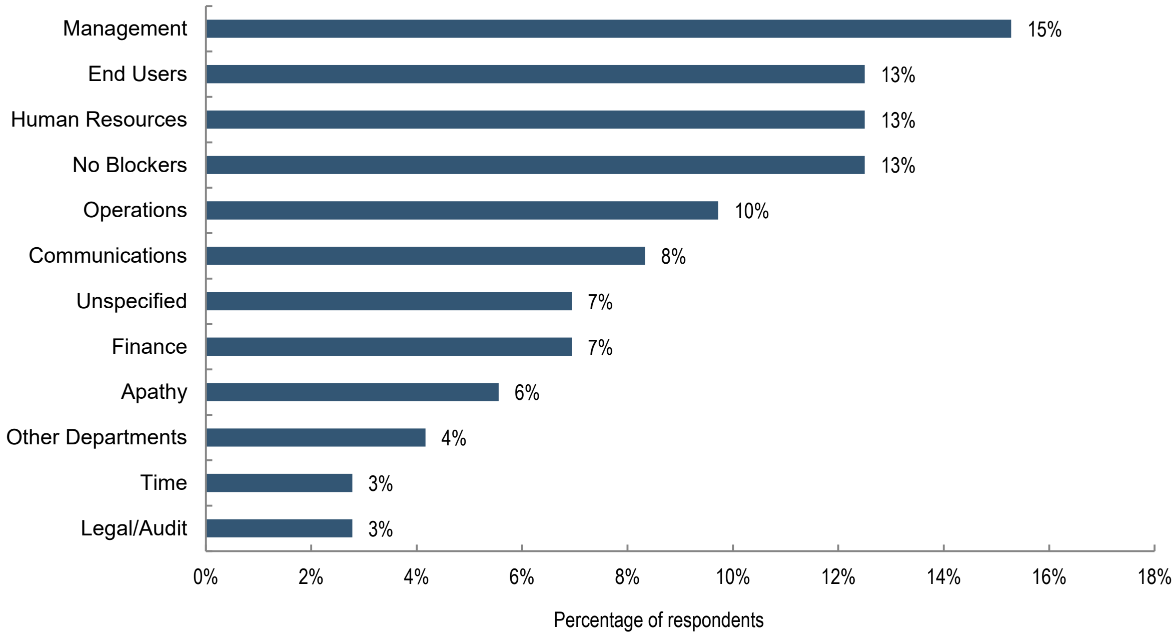

Figure 9. Biggest individual/role blocker to awareness program (n = 72)

Maturity and Metrics

Understanding the maturity of your information security program—and using metrics to measure and convey maturity levels—is critical to demonstrating the value of information security awareness programs. Awareness metrics pose a difficulty, however, in that they typically measure the number of end users that have demonstrated poor security practices or have been the victims of an information security attack or event. If the program is successful, these metrics should signal improvements each year. It is difficult, if not impossible, to measure the number of individuals who did *not* fall prey to a phishing attack or who did *not* commit a security violation. Nonetheless, higher education institutions do attempt to collect some metrics—such as the number of infected devices and number of security violations—that may demonstrate the effectiveness of their awareness efforts if measured over time (see figure 10).

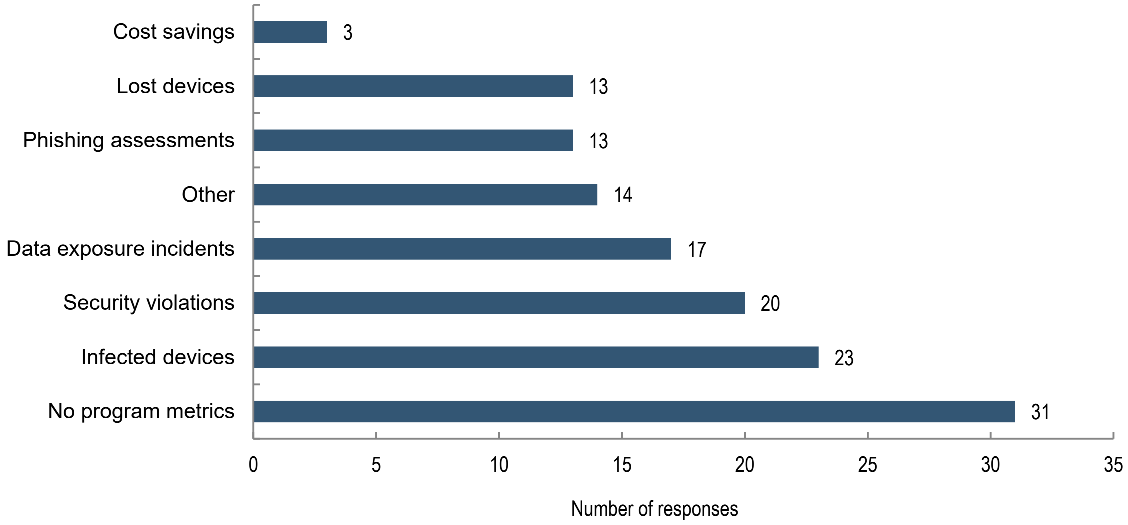

Figure 10. Counts of most common program metrics (n = 70 individual respondents and 133 "check all that apply" responses)

Evaluating the maturity of an institution's information security capability can help an institution determine where it is in delivering a service and where it aspires to be. In 2016, EDUCAUSE introduced a new service that provides capability reports that comprise maturity and deployment indices for information security programs.[13] In the EDUCAUSE Information Security Maturity Index, information security awareness and training activities are included as one element of the security services and operations capability. In 2011, SANS created a maturity model just for information security awareness programs.[14] The SANS model has five maturity stages, moving from a nonexistent program to one that uses a metrics framework to measure awareness program success.

The educational services sector seems to lag behind other industries surveyed by SANS with respect to awareness program maturity (see figure 11). Nearly three times as many respondents from the education sector reported the maturity of their security awareness program as "nonexistent" (17% versus 6%). On the opposite end of the spectrum, none of the education sector respondents said their program is at the highest level of maturity, compared to 2% of respondents from noneducation sectors.

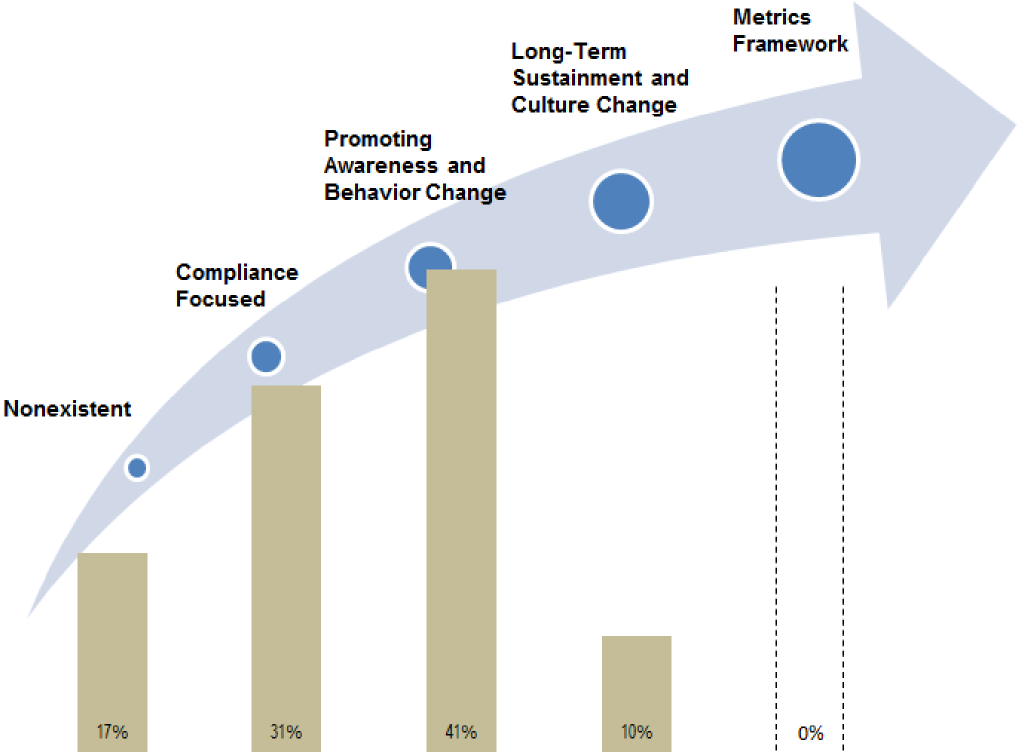

Figure 11. Education sector security awareness program maturity (n = 70)

Rather than focusing on the nuanced differences between sectors, consider a few strategies to increase the maturity of a security awareness program model:

- Confirm executive support for information security awareness and training efforts.
- Designate an individual responsible for security awareness training.

- Ensure that the individual has adequate resources (time and budget) to devote to awareness training efforts.
- Plan security awareness training efforts in a concerted manner.
- Measure the effectiveness of security awareness training efforts in a manner that can be tracked over time.

What It Means to Higher Education

The SANS research, specifically with respect to the educational services sector, shows that 51% of higher education information security awareness programs sit at the third and fourth levels of maturity (on a five-point scale) and that 82% measure at the second, third, and fourth levels of maturity. At the same time, these information security awareness programs seek to promote awareness, change behaviors, and engage in long-term culture change with security awareness professionals who attend to these duties on a part-time basis and have sparsely staffed programs with very limited budgets. Despite those constraints, executive support for higher education information security programs is generally high. That is a good sign because it indicates maturity potential—interest tends to precede priority, priority tends to precedes investment (support), and investment (support) tends to precedes maturity. Education sector respondents with the highest reported maturity level say they have sufficient executive support. Conversely, respondents with the lowest maturity (nonexistent) level report the lowest level of support (see figure 12). Although there is not a statistically significant correlation between maturity level and executive support, the visual depiction of executive support and maturity in figure 12 does show promise that support begets maturity (or the reverse—that showing signs of maturity begets executive support). Never has so much been done with so little.[15]

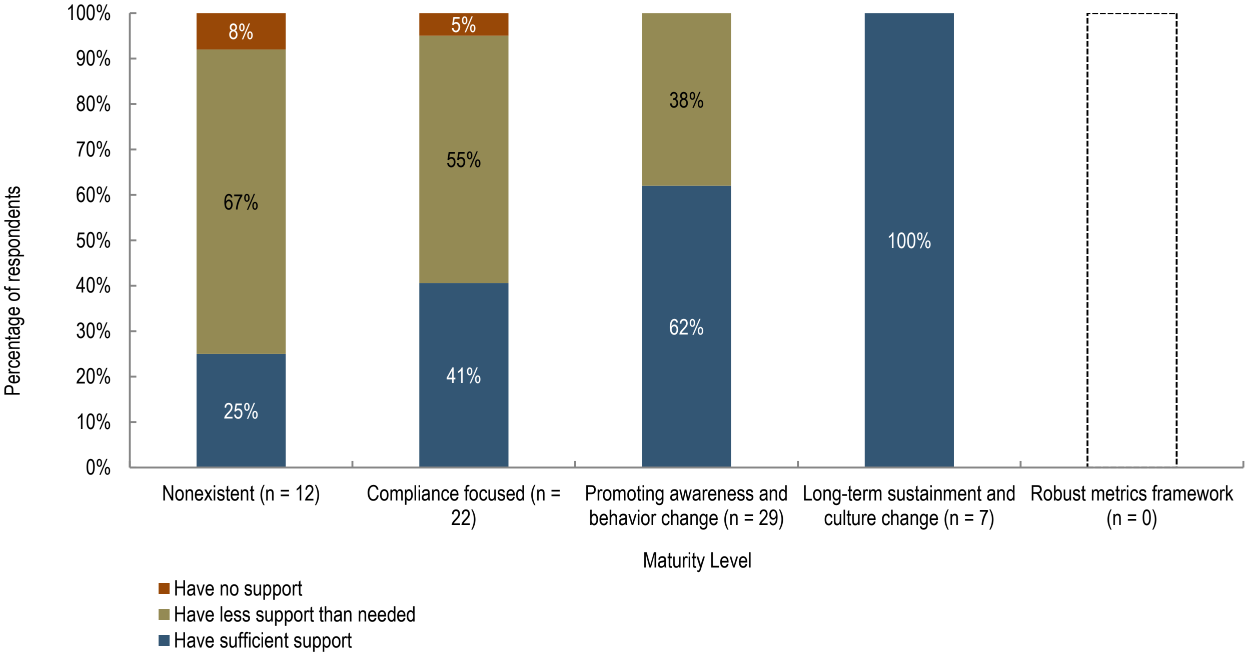

Figure 12. Comparison of level of executive support and program maturity level (n = 70)

Key Questions to Ask

- Who leads your information security awareness and training program? Does that person have sufficient time and resources to attend to awareness and training duties?
- Does your information security awareness and training program have a budget suitable to meet program goals? Is there a plan for how training and awareness activities will be conducted each year?
- Does executive management support your information security awareness and training program?
- Do you measure the maturity of your information security awareness and training program? Are metrics collected to show that the program is successful and proves a return on investment?

Where to Learn More

- Higher Education Information Security Council (HEISC) *Information Security Guide*.
- Higher Education Information Security Council (HEISC) Information Security Guide, "Cybersecurity Awareness Resource Library."
- Higher Education Information Security Council (HEISC) Information Security Guide, "NCSAM Resource Kit."
- SANS Institute, *Awareness Is Hard: A Tale of Two Challenges*, Security Awareness Report, March 2016.
- Woelk, Ben. "The Successful Security Awareness Practitioner." Research bulletin. Louisville, CO: ECAR (forthcoming).

About the Authors

Joanna L. Grama is the Director of Cybersecurity and IT GRC Programs for EDUCAUSE. Eden Dahlstrom is the Chief Research Officer for EDUCAUSE.

Citation for This Work

Grama, Joanna L., and Eden Dahlstrom. "Higher Education Information Security Awareness Programs." Research bulletin. Louisville, CO: ECAR, August 8, 2016.

Notes

1. SANS Institute, *Awareness Is Hard: A Tale of Two Challenges*, Security Awareness Report, March 2016.
2. Because survey responses were anonymized, we were unable to pull only those education sector survey responses that came from higher education institutions. Given the EDUCAUSE promotion of this research, for the purposes of this research bulletin we assume that a majority of the responses from the education sector came from institutions of higher education.
3. EDUCAUSE Benchmarking Service, *Information Security Key Factors*, unpublished.
4. Joanna Lyn Grama and Valerie M. Vogel, "The 2016 Top 3 Strategic Information Security Issues," *EDUCAUSE Review* 51, no.1 (January/February 2016).

5. SANS Institute, *Awareness Is Hard*.

6. Write-in responses for the "Other" category were reviewed and recoded into the existing categories as appropriate. Six responses for the education sector and 13 responses for the other sectors were harvested from the write-in options.

7. EDUCAUSE members understand that higher education training and awareness professionals may be short on time and need easily consumable content to share with their communities. The 2016 Campus Security Awareness Campaign provides ready-made content to support security awareness professionals and IT communicators as they develop or enhance their own security awareness plans.

8. See Ben Woelk, *The Successful Security Awareness Practitioner*, research bulletin (Louisville, CO: ECAR, forthcoming).

9. SANS Institute, *Awareness Is Hard*.

10. 2015 Core Data Service Almanac, *All Non-Specialized U.S. Institutions*.

11. SANS Institute, *Awareness Is Hard*.

12. One of the authors of this document is a lawyer by training.

13. EDUCAUSE Benchmarking Service (beta).

14. SANS, "Defining the Security Awareness Maturity Model," Security Awareness Blog, March 8, 2016.

15. Perhaps this is the unofficial motto of the security awareness practitioner: "We have done so much, for so long, with so little, we are now qualified to do anything with nothing." —Konstantin Jireček