The Successful Security Awareness Professional

Foundational Skills and Continuing Education Strategies

ECAR Research Bulletin | AUGUST 10, 2016

Ben Woelk, Rochester Institute of Technology

Overview

Awareness is an important part of any higher education information security program. In 2015, 74% of U.S. institutions required information security training for faculty or staff, and 27% of institutions required such training for students.[1] Higher education provides an especially challenging environment for security awareness education—along with staff and faculty turnover, we have a large transient student population, making a strategic security awareness plan a requirement for consistent and measurable change. However, the transience of the student population also means it's not easy to measure success year over year. As we get a portion of the target population hardened, we're suddenly faced with an influx of as many as 30% new end users. New requirements, whether internally or externally driven, require skillfully orchestrated change management activities.

Because of these issues, many institutions choose to dedicate an individual to security awareness efforts. How do institutions identify appropriate candidates for this role? How do institutions determine the appropriate qualifications for a successful security awareness professional? What types of educational backgrounds best prepare these professionals? How do security awareness professionals stay current with respect to communications skills, learning pedagogy, and information security issues?

Highlights

In the second half of 2015, the Higher Education Information Security Council (HEISC)[2] Awareness and Training Working Group conducted a survey of security awareness professionals. Although the Awareness and Training Working Group provides support and develops materials for promoting information security awareness on campus, it had not looked closely at the background and continuing education needs of those people providing the awareness training—security awareness professionals.

The research took a two-phased approach: surveying security awareness professionals (and IT communications professionals) and then leveraging the combined expertise of these professionals to provide a rich online resource list of continuing education opportunities. This survey was promoted by EDUCAUSE and had 46 completed responses.

Survey Methodology

The research team consisted of two members of the HEISC Awareness and Training Working Group, who drafted the survey, which was then reviewed by EDUCAUSE communication staff and other members of the working group. The finalized survey was promoted from mid-July to mid-August 2015 to members of three EDUCAUSE constituent groups, who were asked to encourage colleagues to participate as well.

The survey consisted of 22 questions, none of which were required. More than half (12) were open-ended questions. The survey was anonymous and did not collect the respondent's name or contact information.

Respondent Demographics

Our research found that a majority of the survey respondents work at public doctoral research institutions, have college degrees, and hold a variety of security-related certifications. Although not indicated in the survey data, smaller institutions might employ only one security professional, who could focus on program management and technical controls rather than security awareness; this could account for the skewing of the respondent pool toward public doctoral institutions (see figure 1).

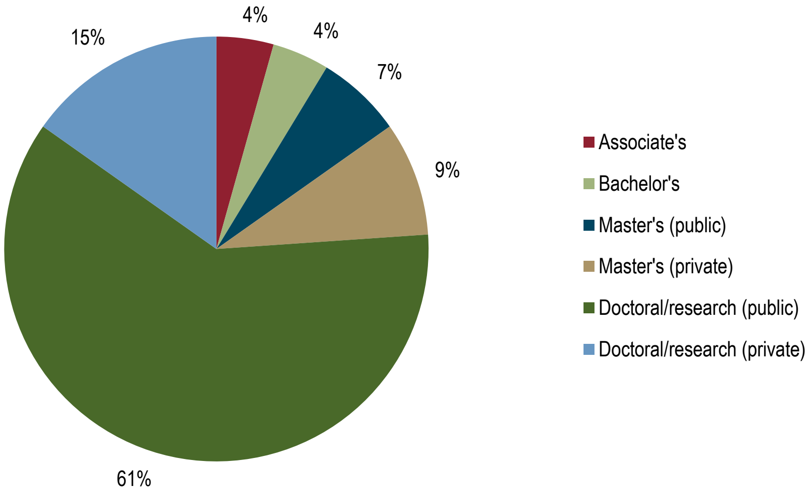

Figure 1. Survey respondents by Carnegie Classification

Although 63% of the respondents indicated responsibility for security awareness and training, more than two-thirds of those respondents said they have responsibility for other information security areas, ranging from forensics to incident response, disaster recovery, enterprise applications and training, and policy development. Few respondents were dedicated entirely to security awareness activities.

- About one-third (37%) of respondents indicated management and/or leadership responsibilities related to information security (11 CISOs, 2 CPOs, and 4 ISOs).
- Only 13% of respondents have titles that include "awareness-related" terms (communication, outreach, awareness).
- Although many respondents indicated they were responsible for developing training, only 24% have formal instructional design training.

As expected in a higher education environment, most respondents hold at least bachelor's degrees, while more than half have earned postgraduate degrees (see figure 2).

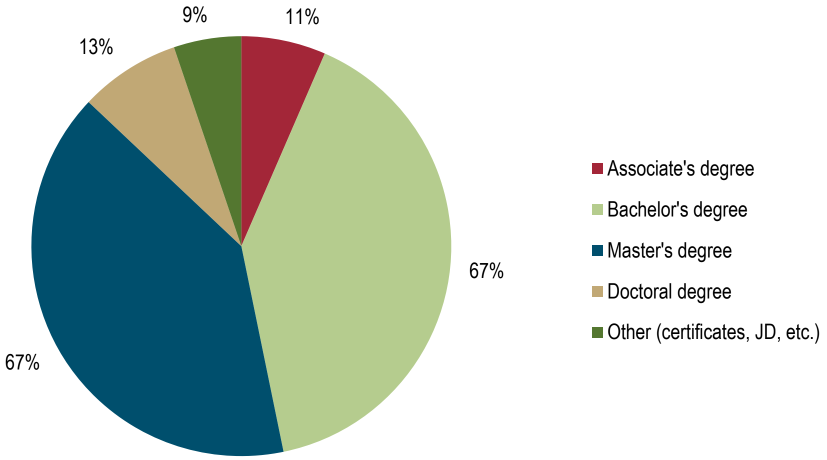

Figure 2. Education level of respondents

Certification and Professional Memberships

Almost all respondents have some type of certification, with 84% holding multiple certifications. Figure 3 represents the most common certifications identified in the survey.[3]

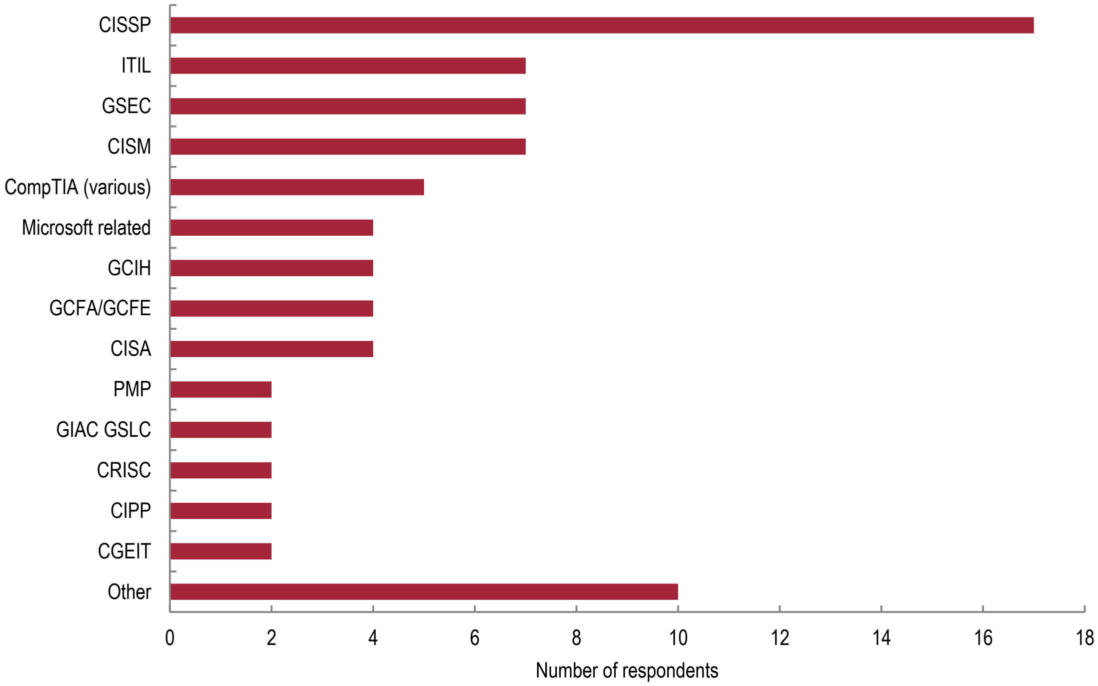

Figure 3. Certifications held by survey respondents

Most of the certifications listed are highly technical. As for other information security professionals, certifications held by security awareness professionals appear to be weighted heavily toward technical knowledge and the appropriate application of controls. Given that a large majority of respondents who indicated responsibility for security awareness have obligations in addition to security awareness (and that 17 are CISOs, CPOs, or ISOs), it's not surprising that so many of the respondents have technical certifications.

Whereas these credentials demonstrate a certain amount of technical know-how, many security awareness professionals would contend that the most difficult awareness challenge is the end user. This is especially true in a higher education environment, with its typical mix of centralized and decentralized information technology, the need to support research, faculty's desire to make their own decisions around their computing needs, and the constraints imposed by FERPA, HIPAA, and other regulations. Although expensive, using technical controls for "target hardening" is relatively easy to implement compared to hardening "soft targets"—end users. Time and time again, attackers obtain credentials and access to systems by phishing or other social-engineering ploys that target end users.

Respondents reported membership in a number of professional organizations. Professional organizations with a clustering of respondents included ISACA, (ISC)^2, InfraGard, and REN-ISAC. Only a few organizations were specific to communications-related skills (Society for Technical Communication and Toastmasters International). Although respondents indicated the value of recently acquired soft skills, for most respondents membership in professional organizations was not leveraged in acquiring those skills (see figure 4).

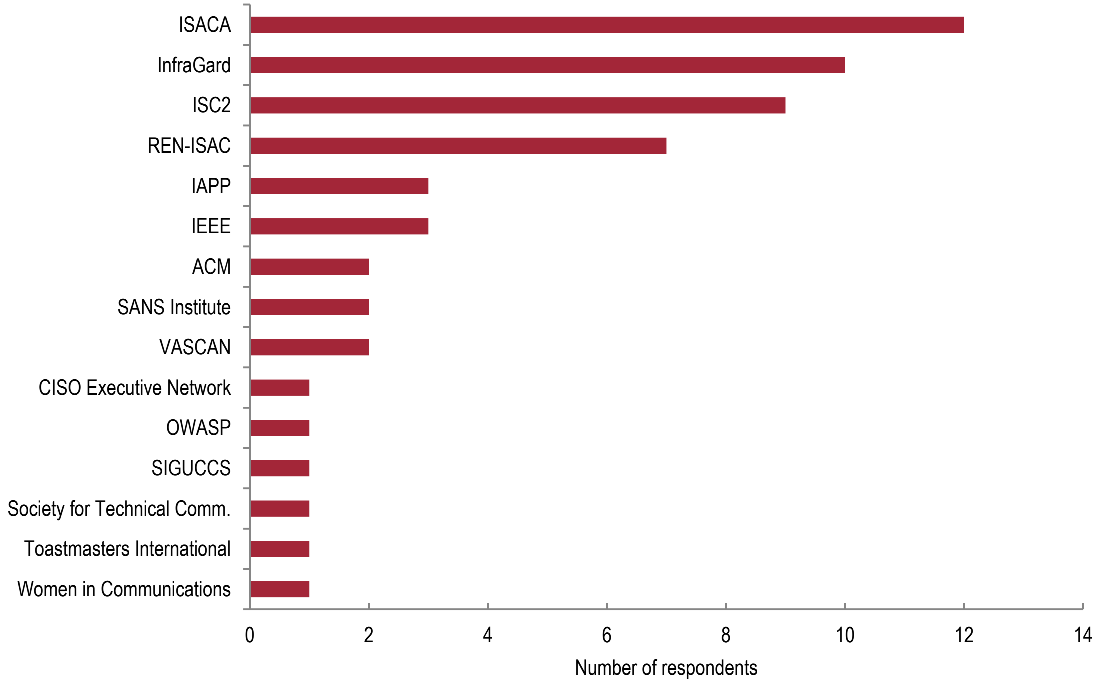

Figure 4. Membership in professional organizations

Experience and Skills

Security awareness professionals are established higher education IT experts. A majority of respondents have worked in the field for 10 years or more, and most have been at their current institutions for at least 5 years. More than 60% of respondents have worked as security awareness professionals—and at their current institutions—for more than five years (see table 1). However, because many respondents have multiple responsibilities, their expertise may be tied to their other IT roles and may not reflect the background of a dedicated security awareness professional. In fact, a large number of successful security awareness professionals may not have technical backgrounds.

Table 1. Survey respondents' experience

Type of Experience	0–1 year	1–2 years	2–5 years	5–10 years	10–15 years	15–20 years	>20 years
Specifically in higher education	1 2.2%	0 0.0%	6 13.0%	7 15.2%	10 21.7%	12 26.1%	10 21.7%
At current institution	2 4.3%	3 6.5%	11 23.9%	8 17.4%	11 23.9%	6 13.0%	5 10.9%
In information security awareness (entire higher education career)	3 6.5%	0 0.0%	14 30.4%	12 26.1%	10 21.7%	6 13.0%	1 2.2%
In information security awareness (current position)	4 8.7%	3 6.5%	20 43.5%	12 26.1%	5 10.9%	2 4.3%	0 0.0%

Four in five respondents (80%) have previously worked in sectors other than higher education. Of these, 38% have worked in government, 22% in the nonprofit sector, 18% in the financial sector, 5% in media, and 17% in other areas.

Respondents identified a number of recently acquired skills that have proven helpful in their roles. Of these skills, more than 70% were in soft-skills areas, such as public speaking, communications/ presentation skills, and relationship building. (Only 20% of the recently acquired useful skills were technical.) Almost 25% of respondents indicated that they have found the development of public speaking skills to be a factor in their effectiveness; other respondents indicated that building relationships is also a helpful skill. Generally, soft skills are an important enabler for awareness and training (and frankly, for success in all roles that include management or that are customer facing; see figure 5).

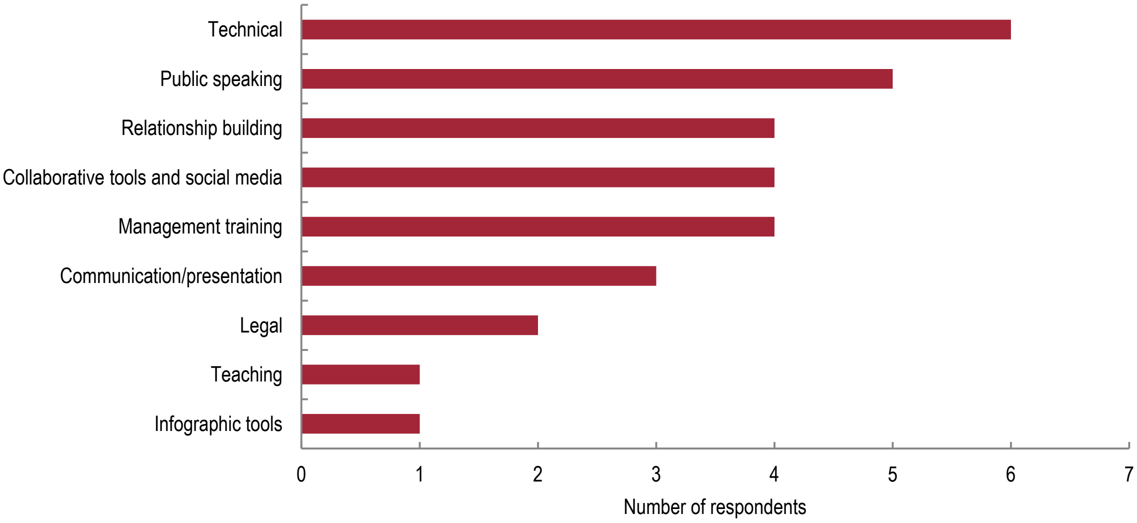

Figure 5. Respondent skills

Almost three in five respondents see value in taking a course to improve technical communication skills specific to security awareness and training, while less than one in five do not see value. (Although not reflected in figure 6 below, the expected cost of that course ranged from $0 to $2,000, with most responses clustered between $250 and $800.)

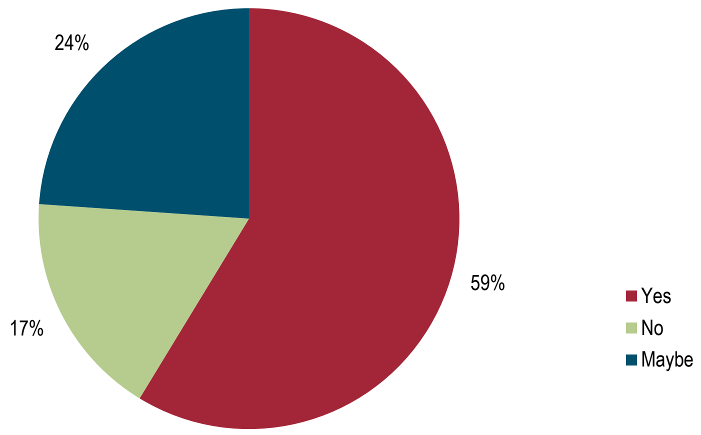

Figure 6. Interest in online technical communications courses

More than half of the respondents (52%) indicated that they were developing e-learning materials. However, less than a quarter of respondents have had formal instructional design or course-development training. Effectively designed training should produce better results. Security awareness professionals would benefit from formal training in instructional design and course development.

What It Means to Higher Education

Being a successful security awareness professional does not require a technical background. Many successful security awareness professionals come from nontechnical backgrounds, with degrees ranging from the liberal arts to instructional design and training. Professionals from nontechnical backgrounds often have stronger communication and interpersonal skills. Coupled with a basic knowledge of information security fundamentals, they can provide effective awareness communication and training to all but the most technical audiences. (With the assistance of technical subject-matter experts, they can develop effective communication and training to technical audiences as well.)

Effective continuing education paths exist for security awareness professionals with technical or nontechnical backgrounds. A successful security awareness professional may need to complement existing knowledge with training/coursework/certification in needed areas.

Professionals with a technical background must maintain that expertise and add coursework or certification in technical communication and instructional design. Professionals with a nontechnical background must add coursework or certification in information security fundamentals, technical communication, and instructional design.

To reiterate, skilled security awareness professionals can produce effective results, but they need continuing education in both technical (hard) and nontechnical (soft) skills. Identifying an effective continuing education path can be a challenge because information security, by and large, is concerned with technical skills and solutions. It's relatively easy to identify a continuing education path focused on technical skills. Scant attention has been given to the development of the soft skills needed to communicate successfully with end users and management.

Many security professionals speak neither "end user" nor "business." IT and security departments must allocate training dollars for training in soft skills as well as in technical skills or technology. Universities and colleges may offer a wealth of resources, ranging from site licenses for recorded training to coursework in areas pertaining to technical communication and instructional design or organizational change.

Awareness and Training Certification Value

The IT profession highly values certifications as demonstrations of competency in a certain field. While no information security awareness and training certification currently exists, the survey asked respondents about the value of such a certification: 35% said it would be valuable, while 26% were unsure (see figure 7).

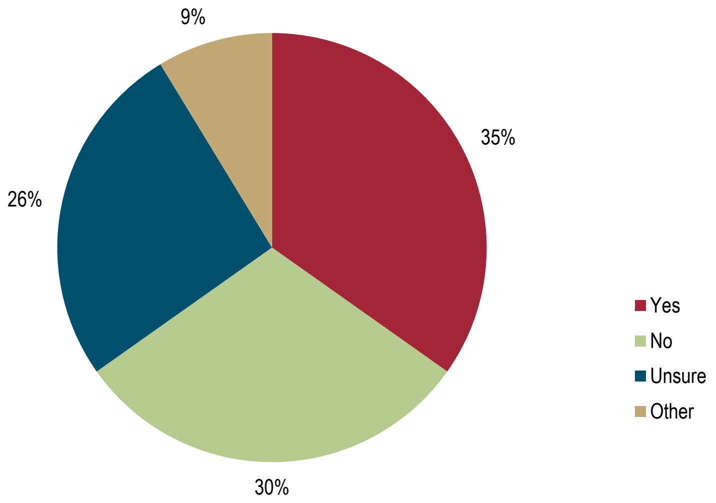

Figure 7. Perceived value of an awareness and training certification

Although the survey did not provide information about what an information security awareness and training certification would entail, the skills needed to be a successful security awareness professional suggest that such a certificate would need to represent evidence of:[4]

- An understanding of basic information security concepts, but not to the level required for the CISSP
- The ability to apply basic technical communication principles, including audience analysis and the ability to manage technical information in ways that allow people to take action[5]
- The ability to apply basic instructional design principles, including analysis of learning need and systematic development of instruction, as articulated by the International Board of Standards for Training, Performance, and Instruction and the Association for Talent Development

Partnerships

Perhaps more frequently in higher education than other industries, security awareness professionals often partner with other institutional resources to produce effective communications (see figure 8). These resources can greatly expand the professional's typical skill set and reach. For example, a security awareness professional might leverage graphic artists working in a university news organization or communications expertise from a dedicated IT communications or media relations professional. A security awareness professional might also leverage subject-matter expertise from teaching or research faculty in computing security and other related areas. A successful security awareness professional will partner with appropriate university resources to provide both communications-related and technical subject-matter expertise.

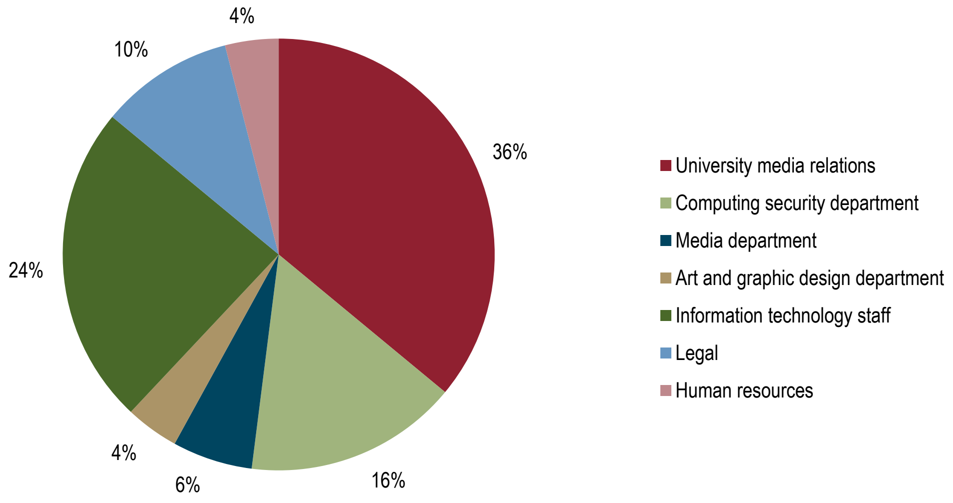

Figure 8. University partners

Key Questions to Ask

- What do I need to learn to become an effective security awareness professional?
- I'm responsible for security awareness, but I come from a technical background. How do I build my soft skills?
- I'm responsible for security awareness, but I come from a nontechnical background. What technical skills do I need, and how do I acquire them?
- What educational resources are readily available where I work that will assist me in my job?
- What additional training will make me more effective as a security awareness professional?

Where to Learn More

- Higher Education Information Security Council (HEISC) *Information Security Guide*, "Successful Security Awareness Professional Resource List."
- Higher Education Information Security Council (HEISC) *Information Security Guide*, "Cybersecurity Awareness Resource Library."
- Joanna L. Grama and Eden Dahlstrom, "Higher Education Information Security Awareness Programs," research bulletin (Louisville, CO: ECAR, August 8, 2016).

Acknowledgments

The author wishes to thank Pat Falcon at Brown University for her tireless assistance with designing and developing the 2015 security awareness practitioner survey and her countless contributions to this research bulletin.

About the Author

Ben Woelk, CISSP, is the Program Manager for the Information Security Office at the Rochester Institute of Technology, where he has developed a leading information security awareness program. Ben is also adjunct faculty at RIT, teaching classroom and online courses in Computing Security Fundamentals and Technical Communication.

Citation for This Work

Woelk, Ben. *The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies*. Research bulletin. Louisville, CO: ECAR, August 10, 2016.

Notes

1. 2015 EDUCAUSE Core Data Service, *Information Security Module*.
2. The Cybersecurity Initiative is led by the Higher Education Information Security Council (HEISC), whose mission is to support higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.
3. You can read about common information security certifications in the HEISC *Information Security Guide*.
4. There are a number of paths to obtaining the requisite skill set to become an effective security awareness practitioner. See the online resource list for recommendations.
5. The Society for Technical Communication breaks this down into nine core skill areas of technical communication: project planning, project analysis, content development, organizational design, written communication, review and editing, visual communication, content management, and production and delivery.