IT Leadership in Higher Education, 2016: The Chief Information Security Officer
**Contents**

- Introduction 3
- Key Findings 4
- The Chief Information Security Officer at the Institution 5
- Scope of Work 9
- CISO Experience Profile 13
- Making Future CISOs 21
- Conclusion 24
- Advice for Current CISOs 25
- Advice for the CISO’s Supervisor 26
- Advice for Aspiring CISOs 27
- Methodology 28
- Acknowledgments 28

---

**Authors**

Jeffry Pomerantz, EDUCAUSE Center for Analysis and Research
Joanna Grama, EDUCAUSE

**Citation for This Work**


©2017 EDUCAUSE. Creative Commons BY-NC-ND 4.0.
Introduction

Information technology supports the core institutional missions of teaching, learning, and research and is a critical part of the infrastructure of the institution. Yet that infrastructure is constantly changing as technology evolves, which presents a constantly shifting set of risks to the institution. Information security policies and practices that deal with issues such as access control, data breaches, and compliance are therefore more urgently needed than ever. It is critical for an institution to have an effective information security leader who can address these issues on many levels, from communicating the issues with top stakeholders to establishing and maintaining an effective institution-wide information security program. With the demand for information and technology security growing, understanding how information security professionals can best lead in these efforts is vital for an institution to succeed.¹

As part of its series of studies of the IT workforce in higher education, the EDUCAUSE Center for Analysis and Research (ECAR) conducted a survey of chief information security officers (CISOs). This study sought to identify the characteristics and functions of CISOs: What background and training do these individuals possess, what is their scope of work and responsibilities, and what personal and professional characteristics contribute to their success? The audiences for this report are CISOs themselves, those who aspire to be CISOs, and those to whom CISOs report. This report can help all of these stakeholder groups understand the job of the CISO—at their local institution and elsewhere—and compare it with a higher education–wide “baseline.”

EDUCAUSE IT Workforce Research: Focusing on Our People and Professions

This report is part of the IT Workforce in Higher Education, 2016 research series, which includes IT leadership reports on the chief information officer, the chief information security officer, the enterprise architect, and the chief data officer. These practical reports analyze the skills needed to prepare for and fulfill functional roles and are intended for aspirants, those in the roles now, and their IT managers and leaders. The research helps colleges and universities reinvest in the IT workforce by defining professional competencies and laying the foundation for tools that can guide professional development and career planning.
Key Findings

- **CISOs overwhelmingly report to the CIO.** CISOs disagree, however, on whether the ideal reporting relationship is to the CIO or to the president or chancellor.

- **The leadership position to which CISOs believe they should report varies depending on how the CISO believes information security leadership should be projected on campus.** CISOs who think they should report to the CIO value the integration this enables with the IT infrastructure and leadership on campus; CISOs who think they should report to the president or chancellor value the separation from IT and the influence this provides across the institution.

- **CISOs’ responsibilities fall into three major areas:** protecting the institution’s IT systems and the data contained in those systems, maintaining the institution’s information security infrastructure, and acquiring information security systems and coordinating with vendors.

- **Many CISOs would take on additional areas of responsibility, and few would give any up.** This reflects the importance of all areas within CISOs’ scope of responsibility to information security in institutions of higher education.

- **CISOs spend some time on most activities within their scope of work, though no single activity dominates.** This finding indicates that all CISOs spend time “in the trenches.”

- **CISOs have been at their current institutions for a median of 10 years and in higher education even longer.** Given that CISOs are among the youngest IT leaders, they have been at their current institutions for a significant percentage of their working lives.

- **Diversity is a major issue for CISOs, as it is for security positions generally.** In particular, women face many obstacles in the IT professional pipeline.

- **CISOs are overwhelmingly hired from within their current institution.** CISOs primarily come from other information security positions, secondarily from other positions that are technically oriented but not explicitly focused on information security.

- **CISOs have responsibility for many areas of information security in which they do not believe they are experts.** On the other hand, CISOs have positive views of their performance in the essential roles that an information security leader plays.

- **CISOs consider information security to be a service that is provided across all areas of technology and operations at an institution.** This requires that the position often be more about institutional strategy and politics and projecting leadership on campus than about technical skills.
The Chief Information Security Officer at the Institution

EDUCAUSE has been studying the CISO position for well over a decade. One early study by ECAR found that the CISO position first appeared in higher education in 1994, though of course some institutions and types of institutions were earlier adopters than others. Indeed, this adoption is still under way; according to the EDUCAUSE Core Data Service (CDS), only 34% of institutions have a dedicated employee whose primary responsibility is information security.

Job Titles

Early ECAR studies in 2003 and 2006 found a wide range of positions that had day-to-day responsibility for information security, from the CIO to the chief IT security officer to the director of networking. In 2003, only 22% of institutions had a position with the title chief IT security officer, which lagged behind other job titles with day-to-day responsibility for information security. By 2006, the title IT security officer had overtaken other job titles with responsibility for information security, though still only at 35% of institutions.

The current survey asked for responses from “the highest-ranking information security leader” in the IT organization. As these previous studies make clear, there is great variety in the titles of information security leadership positions. Respondents were therefore asked to select the position titles that best align with their current information security leadership role. The most common position titles were CISO (62%), information security officer (26%), and director/lead, information security (19%). While most selected only one title, respondents could select all that applied from the list of titles, and about one-fifth selected more than one title. The most common combined titles were CISO and director/lead, information security.

The vast majority of respondents (83%) believe that their current title accurately reflects the scope and nature of their responsibilities. The most common perceived mistitle is among information security officers, who believe they should hold the title of chief information security officer. This seems a reasonable criticism, if the information security officer is indeed the highest-ranking information security leader on campus—which they clearly are, as most information security officers report to the CIO. Certainly having the word chief in one’s job title signals the importance of the position and lends weight to the influence one needs to be successful in the role.
Reporting Relationships

Indeed, whatever title the highest-ranking information security leader on campus has, this position overwhelmingly (82%) reports to the CIO or equivalent position. A slim majority (52%) of respondents who report to the CIO agreed that this is the appropriate reporting relationship for them to have... but that of course means that 48% believe they should report to a position other than the CIO. This 48% is highly fragmented. The largest subgroup consists of those who believe they should report to the president or chancellor (46% of those who report to the CIO but believe they should not); the remaining responses are spread across many leadership positions. These actual and desired reporting relationships are shown in figure 1.

**Figure 1. To whom CISOs report and think they should report**

Why are the CIO and the president/chancellor the positions to which most CISOs believe they should report? Following the question about which position respondents think they should report to, respondents were asked why they think so, and the responses to this question are illuminating. Several CISOs who report to the CIO and think this is the appropriate reporting relationship pointed out that IT and information security are tightly linked and that, of all campus leaders, the CIO is best able to use the information provided by the CISO to influence decisions and decision makers on campus to prioritize information...
security. A few CISOs also suggested, however, that in order to be effective in this influence, it is critical that the CIO have a strong understanding of the campus IT environment and the risks inherent in IT and also be committed to information security. On the other hand, one CISO who reports to the president and thinks this is the appropriate reporting relationship suggested that the influence on decisions and decision makers on campus to prioritize information security should come from the top. Several CISOs who report to the CIO but think they should report to the president/chancellor reiterated this sentiment, suggesting further that information security is not confined to IT and must be embraced by institutional policy. These respondents suggested that there is an inherent tension between the work of the CIO and the CISO: Whereas the CIO’s role is to deliver services to the campus community, the CISO's role is to manage the risks that those services may present. In short, CISOs who think they should report to the CIO value the integration this enables with the IT infrastructure and leadership on campus, while CISOs who think they should report to the president/chancellor value the separation from IT and the influence this provides across the institution.

Regardless of how much influence the CISO’s manager has, most CISOs have little formal influence, either in the number of staff members reporting to them or in their membership on institutional leadership bodies. About a fifth of respondents have no reports, either direct or indirect, and 53% have five or fewer total reports, a finding consistent with 2016 data from CDS, which shows that across all U.S. institutions, central IT units have only 0.2 full-time information security employees (FTE) per 1,000 institutional FTEs, a figure that may include the CISOs themselves. On the other hand, 29% of respondents have 10 or more total reports. The median number of total reports that CISOs have, overall, is 5, but one of our respondents has over 100 total reports. This many reports seems to indicate a department, a conclusion supported by the fact that this respondent is a CISO at a very large doctoral institution. Interestingly, respondents with the title CISO have significantly more employee supervision responsibilities than those with other titles: a median of seven total reports for CISOs versus a median of two for other position titles.

CISOs also have little formal influence over their institution’s leadership. Only 7% of our respondents are members of the president’s or chancellor’s cabinet at their institution. Worse, only 1% of respondents are expected to attend every meeting of their institution’s board of regents or board of governors, though 43% attend on an as-needed basis. Given the nature of the CISO role, “as needed” may mean to report about a recent information security incident at the institution. When CISOs do attend board meetings, 61% must have their updates approved in advance by the CIO, and 16% by other institutional leaders, lending credence to the interpretation that CISOs mostly speak to the board to relay bad news.
The picture that emerges of the CISO role is complex: A wide majority of CISOs report to the CIO or equivalent, even as a strong case can be made for CISOs to report to the president/chancellor. The CISO manages few staff, but, as one might expect, this tends to increase at larger institutions. Also, the CISO generally has little contact with institutional leadership, and what contact there is must often be cleared by other institutional leaders. Given these limitations, one might expect CISOs to feel hampered in their influence at the institution, but by and large this is not the case. Most CISOs said they have significant influence at their institution. Where does this influence come from? In part, it comes from the CISO’s broad scope of responsibility.
Scope of Work

In July 2000, the higher education information security community banded together to support one another professionally by founding the Higher Education Information Security Council (HEISC). Today, the mission of this community is "to support higher education institutions as they improve information security governance, compliance, data protection, and privacy programs." Part of this support has been the development of an extensive higher education Information Security Guide. This guide contains, among other things, toolkits for CISOs at all stages of their careers, resources on a wide range of information security–related topics, and case studies of information security solutions implemented by specific institutions. In short, the guide articulates and explores many of the areas within CISOs’ broad scope of responsibility. This scope will naturally vary across institutions and types of institution. But as the guide makes clear, there are information security programs and practices that are particularly relevant in the context of higher education. This section explores the specific tasks that are within our respondents’ scope of responsibility.

Areas of Responsibility

Respondents were asked a set of three questions about their responsibilities, with identical lists of 18 possible responses (plus an “other” option). These response options were information security program areas identified by HEISC volunteers:

- What areas of information security are you currently responsible for at your institution?
- Are there any areas of information security that you are but should not be responsible for at your institution?
- Are there any areas of information security that you are not but should be responsible for at your institution?

Figure 2 shows the overall responses to all three of these questions. Notably, CISOs’ responses to the question about current scope of work fall into three rough groups. The first group, for which 90% or more of CISOs have current responsibility, consists of six items: information security policies, awareness and training, incident management, information security compliance, organization of information security, and risk assessment and management. These items make a reasonably well-defined responsibility set, which includes developing policies and processes to address information security risks, managing actual information security incidents, and educating the campus community about information security hygiene. In other words, CISOs overwhelmingly have responsibility for protecting the institution, its IT systems, and the data contained in those systems and for managing information security incidents when safeguards fail. Indeed,
“ensuring that information security incidents do not occur and managing them when they do” may be a reasonable brief description of the job of CISO.

The second group, for which 55–65% of CISOs have current responsibility, consists of eight items: operations security, data privacy, supplier relationships, communications security, identification and authentication, cryptography, contingency planning, and access control. Most of these items make a well-defined responsibility set around managing information security and compliance requirements for critical operational infrastructure, whether that infrastructure is on campus or in the cloud. The third group, for which a third or fewer of CISOs have current responsibility, consists of four items: system acquisition, development, and maintenance; human resources security; asset management; and physical and environmental security. A minority of CISOs are responsible for at least some of the work involved in acquiring IT systems, as well as for vetting the users of campus systems for appropriate access levels and the

Figure 2. CISOs’ current and ideal scope of responsibility
physical environments in which these systems are placed. All of these areas of responsibility support areas in the first responsibility set, discussed above—preventing and managing information security incidents.

The second question, areas of information security that the respondent is but should not be responsible for, received far fewer responses. Indeed, only three areas received five responses; the rest received even fewer. These three areas are data privacy, supplier relationships, and contingency planning. It is perhaps understandable why CISOs might believe they should not be responsible for these areas. Supplier relationships and contingency planning may more appropriately be the responsibility of the CIO, the former because the CIO has budget and contract responsibility for a central IT unit, the latter because the CIO has primary responsibility for the operation of all IT systems on campus. Data privacy, on the other hand, may more appropriately be the responsibility of the individual or campus unit that generated or owns the data or is otherwise responsible for dealing with specialized laws concerning the use of data. Campus medical centers, for example, are responsible for compliance with the Health Insurance Portability and Accountability Act. Furthermore, while security and privacy overlap, they are not the same, and data privacy may more appropriately be the responsibility of the institutional privacy officer, a position often separate from the CISO.15

The third question, areas of information security that the respondent is not but should be responsible for, received quite a large number of responses. Indeed, almost all of the listed areas of information security received at least one response. On the one hand, it would be easy to see this as a desire for a land-grab by these CISOs. On the other hand, this may reflect a recognition by CISOs that applying information security policies and practices in these areas could lead to positive outcomes for the entire institution, a conclusion that is supported by the fact that all of these areas are specifically mentioned in industry standards and best practices devoted to the practice of information security. In conclusion, while all areas of information security are the responsibility of some CISOs, no areas are the responsibility of all CISOs. That many CISOs would take on additional areas of responsibility and few would give any up may reflect that all of these areas are critical to information security in institutions of higher education.

**Time on Tasks**

The 18 possible response options to the questions about areas of responsibility were aggregated into a smaller set of 7 broad activities (plus an “other” option) to which CISOs may allocate time. Figure 3 presents the amount of time allocated by CISOs to these various activities. The median is the amount of time spent by the “typical” CISO, while half of all CISOs are contained between the first and third quartiles.

Many CISOs would take on additional areas of responsibility and few would give up any. This may reflect that all of these areas are critical to information security in institutions of higher education.
CISOs do not spend much time on any of these activities, but they spend some time on each of them. This is an especially interesting finding, given the varying number of reports that CISOs have. One might expect that the more reports a CISO has, the less time he or she would spend on certain tasks; these findings indicate, however, that all CISOs spend time “in the trenches.” Furthermore, it is remarkable just how consistent these findings are. The median amount of time that CISOs spend on these activities is quite similar, and the maximum amount of time for most of these activities is under 50%. The only two activities on which any respondents spend more time are security leadership and security incident response, on which one CISO spends 70% and another spends 80% of their time, respectively. Spending a great deal of time on information security leadership may indeed be a keen strategy: If a CISO is a strong leader in this area, others will come to appreciate the value in information security measures and the CISO may thus not need to spend as much time on other activities. Spending a great deal of time on incident response, on the other hand, may reflect a staffing issue. The CISO may have few staff or may be one of only a few individuals who have the expertise or authority necessary to deal with issues around information security incidents, such as collecting computer forensic evidence or speaking directly with law enforcement officials.
CISO Experience Profile

CISOs spend time on all of these high-level activities. This, however, raises the question of what experience is required to be able to perform these disparate tasks. This section investigates the characteristics of the individuals in the CISO role. Who are these individuals, and what is their background? What skill sets do they possess that enable them to perform this role?

Background

CISOs are, demographically speaking, a homogeneous lot. CISOs are predominantly white and male: 84% white, 83% male, 72% both. There is some variation—though not statistically significant—across institution types, however. While only 5% of CISOs are nonwhite at master’s institutions, that number is 17% at doctoral institutions. Diversity is a major issue for CISOs, as it is for security positions generally. Our findings indicate a possible increase in ethnic diversity with the new generation of CISO hires—12% of Boomer CISOs are nonwhite, but 21% of GenX CISOs are nonwhite—though, again, this is not a statistically significant difference. And our findings actually show a decrease in gender diversity—25% of Boomer CISOs are women, but only 12% of GenXers are. This may not be an indication that fewer younger women are going into information security professions, however, but rather an indication of the obstacles that women face in the professional pipeline, particularly in technical positions. This speculation is supported by the data: The median age for male CISOs is 48, while the median age for female CISOs is 54. See figure 4 for the intersections of sex, age, and ethnicity among CISOs.

Figure 4. Demographics and diversity among current CISOs
The overall median age of respondents is 49 (with a range from 28 to 69), which is on the young end of the age range for IT leaders surveyed by ECAR. Perhaps because CISOs are, by and large, younger than other campus IT leaders, they have had less time to earn graduate degrees. A master’s is the highest degree earned by 55% of CISOs; another 30% have solely a bachelor’s.

Pursuing graduate degrees is not the only professional education option for CISOs. Fifty-three percent of CISOs said they intend to earn another certification within the next five years. Unsurprisingly, this figure varies widely by age—65% of GenX CISOs intend to earn another credential, but only 38% of Boomers do. The most highly sought-after credentials by our respondents are the Certified Information Security Manager (CISM) certification and the Certified Information Systems Security Professional (CISSP) certification. Again, this breaks down by age, with 42% of GenXers aspiring to earn the CISM, as opposed to 32% of Boomers. Interestingly, 78% of GenXers (but only 56% of Boomers) already have the CISSP. It is clear that younger professionals in information security are well aware of the salary benefit of certifications and the extent to which hiring committees look for certifications on applicants’ resumes, and they are actively seeking more of those credentials. Furthermore, that so many respondents intend to earn certifications—which demonstrate technical competence—is an opportunity for professional development for CISOs seeking further leadership roles.

**CISO Career Trajectory**

The higher education IT workforce landscape study found that many institutions like to “grow their own” leadership by grooming employees over their career at the institution to fill progressively higher positions. This is especially true for CISOs. The previous position held by 52% of CISOs was at their current institution, and the position prior to that was at the same institution for 30%.

Given that such a large percentage of CISOs are hired from within, what positions should institutions look to for potential future CISOs? Many CISOs’ previous positions were information security–related positions of some variety. The most common previously held positions by current CISOs are director of information security and information security officer, which may be either the second in command to the CISO or the senior-most information security officer for an academic unit. Yet these previous positions account for less than a quarter of current CISOs. Other positions previously held by current CISOs include some that are technically oriented—such as systems administrator and IT consultant—but not explicitly focused on information security. A background in information security is the obvious experience for hiring committees to look for when hiring a CISO. But given that information security is a concern for all IT systems, it may
be worthwhile expanding a search to encompass individuals who may have the requisite experience but not the job title to reflect that fact.

A fairly sizeable percentage (17%) of CISOs were hired to the position from IT executive leadership positions (for example, chief technology officer or associate information officer). But a great many other CISOs, fully 64%, aspire to IT executive leadership for their next position. Indeed, 28% of CISOs aspire to be CIO next. Figure 5 shows, in broad brushstrokes, the categories of the previous two positions held by current CISOs, as well as the categories of the next two positions that current CISOs aspire to. Given the scope of experience and degree of leadership required by CISOs, combined with the fact that many institutions like to “grow their own” leadership, it would behoove search committees seeking CIOs to look to the CISO ranks.

Figure 5. CISOs’ career trajectory

The IT workforce landscape study found that IT managers have been at their current institutions for a median of 12 years. The current study finds that CISOs have been at their current institutions for a median of 10 years and in higher education for a median of 16 years. This is a fairly impressive number; given that CISOs are among the youngest IT leaders, these individuals have been at their current institutions for a significant percentage of their working lives. Current CISOs have worked in information security for a median of eight years and in their current position for a median of three, though a rather remarkable 12% have been in their current position for a decade or more. The institutions at which these long-lived CISOs work span the range of Carnegie types, sizes, and public/private control. One wonders if there are interesting stories among these early adopting institutions, reflecting the evolution and maturation of the practice and field of higher education information security.
Figure 6 presents the median and the middle half of the number of years CISOs have worked in various positions.

Skills

Given the length of time that many CISOs have worked in information security, and the even greater length of time in higher education, they have had opportunity to gain experience in a wide range of areas. Information security–related work requires an extremely wide range of skills; as a result, several questions were included in this study to identify the state of CISOs’ actual skills in these areas. Respondents were asked several questions about the importance of various skills for an information security leader in higher education and about their level of expertise in and experience with several IT sectors.

Respondents were first asked to rate their level of experience in the areas of information security from the questions, discussed above, about CISOs’ areas of responsibility. It is perhaps unsurprising that the order in which CISOs rated their experience maps closely to their areas of current responsibility. After all, having responsibility for something is precisely what gives one experience with it. Indeed, CISOs rate their experience highest in five of the six areas of information security for which 90% or more of CISOs have current responsibility: information security policies, awareness and training, incident management, information security compliance, and organization of information security.

More noteworthy is what is clearly visible in figure 7, which represents some of the same data as figure 2—specifically, the number of CISOs who have current responsibility for certain areas of information security. But figure 7 presents a different perspective on those data. Of the CISOs who have responsibility for an area, what fraction evaluate their level of experience in that area as
sufficient? What figure 7 makes clear is that across the board, CISOs have responsibility for areas of information security in which they believe they need more experience. Indeed, the most common response option for nearly every single area of information security was "some experience; more needed." Perhaps a lack of hubris is a trait of CISOs. More likely, these responses indicate that there are many opportunities for organizations providing information security professional development.

Figure 7. Current responsibilities and expertise of CISOs

In 2016, HEISC and ECAR published a report that presents a model (reproduced in figure 8) of the higher education CISO, including the essential roles an information security leader plays and the skills necessary to fulfill those roles. The core CISO roles reported in this research (strategist, technologist, and trusted advisor) are the underpinning and base of the information security leader and form the first ring in the model. Primary roles, which form the second ring, are those that take the most time to develop; these include the visionary, promoter/persuader, and relationship builder roles. The last green ring in the model represents discrete roles that a CISO may play only at specific times, such as master communicator, coach/mentor, team builder, and change driver.
CISOs consider it important for a successful higher education information security leader to master almost all of these roles. Indeed, almost all roles were rated as very or extremely important by 70% or more of CISOs. The only exception was technologist, which evenly split respondents, with exactly 50% rating it as very or extremely important; a further 41% rated technologist as only moderately important. This is a curious finding, given the deeply technical nature of information security work generally. While CISOs do not consider technologist to be an important role for them to play (perhaps because they have
staff to take on technical tasks), they believe that they possess a high level of technical skill. This may reflect the career path that CISOs have taken to arrive at their current position. Recall that many CISOs come from a background in other information security positions. Also note that the roles trusted advisor, relationship builder, and master communicator were rated the most important. This would seem to indicate that CISOs consider their role to be far more about institutional strategy and politics and projecting leadership on campus than about technical skills.

The HEISC/ECAR report also articulates a set of skills that are not specifically related to information security but are nevertheless needed for each of the roles identified in the model of the higher education CISO. Two survey questions were based on these skills. These questions had identical sets of response options, first, about the importance of a set of skills for an information security leader in higher education to be successful in the role and second, about the respondent’s level of expertise in each of those skills. Figure 10 presents the findings from these two questions. Of note in figure 10 is that CISOs consider almost all of these skills to be important. Indeed, all items were rated as very or extremely important by at least two-thirds of CISOs. Unlike the findings shown in figure 7, however, here CISOs evaluated their level of expertise quite highly. Even so, CISOs’ self-reported level of expertise is consistently lower than their assessment of the importance of skills.
The four skills with the largest gaps between importance and expertise are negotiation, ability to set and manage expectations, oral communication, and ability to influence. The latter three of these are articulated in the HEISC/ECAR report as skills needed for multiple roles played by an information security leader—the roles shown in figures 8 and 9. These roles are broad and, while not all CISOs play all of these roles, they are intended to be more or less universal. This makes the juxtaposition of figures 9 and 10 especially interesting. Figure 9 shows that CISOs have a great deal of confidence in their mastery of these essential roles. Yet figure 10, which breaks out specific skills necessary to fulfill those roles, shows that CISOs have less confidence in their expertise in those skills. In other words, CISOs are critical of their own expertise in several skills necessary for the leadership and political aspects of the position. As with figure 7, either modesty is a trait of CISOs, or there are many opportunities for professional development in the field of information security.

![Figure 10. Expertise in various skills and their importance for success](image-url)
Making Future CISOs

HEISC was established in July 2000 “to support higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.” The community continues to grow. For example, as of this writing, there are almost 3,300 subscribers to the HEISC Security Discussion LISTSERV, where discussions are vibrant and wide-ranging. Additionally, the annual Security Professionals Conference has grown from a workshop of 100 participants in 2003 to a sold-out event with more than 600 attendees on its 15th anniversary. Of course, not every individual interested in information security topics is necessarily a CISO or equivalent position; plenty of CIOs and chief privacy officers (CPOs), for example, participate in community discussions, and it’s easy to understand their interest.

The position of CISO has been widely adopted in higher education. The position is, in fact, one of the most widely adopted of the IT leadership positions studied in ECAR’s current research into the higher education IT workforce. According to data collected by CDS, 34% of institutions of higher education have a CISO-equivalent position, and, as mentioned above, 62% of our respondents have CISO as their job title. Given both this widespread adoption and the large number of institutions still trailing in this adoption, there is a clear need for CISOs now and in the future. Developing new CISOs should therefore be a collective priority across all of higher education. Along with the background and skills possessed by CISOs, of interest too is what these individuals believe is best and most important about the job. Aspiring CISOs, take note.

Respondents were asked what they enjoy most about being an information security leader, and their answers focused on a few important themes. First and foremost was the ability to effect change and exert influence at the institution. The change that respondents seek is specifically to “improve the security posture” of the institution and spearhead “continuous data security improvements.” In other words, CISOs enjoy being able to help define and implement the institution’s information security agenda while enabling the institution’s teaching and research mission, and not, as several respondents explicitly pointed out, “just being the people who say NO.” Improving the institution’s information security posture requires that CISOs educate campus stakeholders about the need for appropriate information security practices and how “to recognize cybersecurity risks.” But it also requires that CISOs continually reeducate themselves because the technology and threat environment are always evolving. Several respondents wrote that this constantly changing environment is a challenge but is precisely what “keeps the interest up.” Indeed, more than one respondent used literally the same phrase: “Never a dull moment.” This constant change, however, means that
the CISO “can influence anything that impacts the campus because everything has some impact on IT, and that means security affects it all.” This, for many respondents, is what makes the job fulfilling.

Working in an environment of constant change is, of course, extremely demanding. Respondents were asked to identify one thing about themselves that they would change to make themselves more effective as an information security leader. Several respondents wrote that they would like to have more patience with the slow rate of change at institutions of higher education, a lament probably shared by many higher education leaders. Another common challenge, and not just in higher education, is the need for more resources, both time—to perform one’s work, learn, and network—and personnel. One Jedi of a respondent even suggested creating a clone army. More realistically, other respondents suggested hiring an assistant and learning to delegate better. Indeed, developing leadership skills was a common theme of many responses to this question, not just down the organizational hierarchy but up and across it as well, which is consistent with the findings presented in the previous section. Many CISOs wrote that they would like to develop a stronger presence on campus, with the CIO and other campus leaders as well as with other campus stakeholders generally. Gaining greater visibility on campus, respondents suggested, would help them be more effective advocates for information security policies at the institution. Interestingly, however, several respondents suggested that a major hurdle to this greater visibility is their innate introversion as “natural technologists.” One CISO even wrote that he should have “focused more on the ‘soft skills’ needed to be an information security leader sooner in my career.”

In that vein, respondents were asked what advice they have for those aspiring to become information security leaders. Unsurprisingly, soft skills emerged as one of the most common responses. Indeed, CISOs are refreshingly blunt on this subject. One respondent wrote that soft skills “are what will help you to succeed,” while another suggested that they are “far more valuable and durable than technical skills.” Indeed, yet another recommended that one should learn soft skills first because “the hard skills are much easier to develop.” This could be taken as a comment on the importance of graduate degrees for success as a CISO as a means to gain those soft skills, as opposed to certifications, which often focus on technical skills.

While CISOs consider soft skills to be critical, technical skills are still important. One respondent wrote that “knowing the technology is important for credibility,” both with campus leadership and others in the information security profession. Credibility appeared several times in CISOs’ advice. Credibility in technical matters is important but is only a starting point. To gain that technical credibility, some respondents suggested getting a certification or other credential.
Beyond that, however, credibility comes from being in tune with the institution’s business operations and strategic direction. This is critical, several respondents suggested, for gaining buy-in from institutional leadership for information security advances. Also critical for gaining buy-in from leadership are skills in networking and institutional politics, which are, according to one respondent, “two of the most important skills for this job . . . it’s very hard to be an infosec leader without buy-in, and those skills go a long way to reaching that critical buy-in.” Indeed, another respondent stated flatly that one must “get buy-in or you won’t get anything done.” And given that getting things done in the information security sphere involves a complex and dynamic set of technologies and stakeholders, all of these many technical and political skills are critical.
Conclusion

Information security routinely appears in the EDUCAUSE annual Top 10 IT Issues list, several times taking the top spot. The importance of information security work to institutions of higher education is undeniable, and especially so at a time when the information security of institutions of higher education is literally a matter of national security. Yet those who do information security–related work—not just in higher education but in all types of organizations—often face an uphill battle. Many factors influence users’ noncompliance with organizational information security policies, and those who do information security–related work for organizations fight the reputation of being, as one respondent to this study wrote, “the Department of No.”

Yet services that constrain more than they enable tend to be ineffective. Providing the service of information security to campus stakeholders requires, as another respondent wrote, “not saying no, but rather saying how”—how to enable campus stakeholders to use the technology and perform the functions they need while mitigating the risks inherent in the use of those technologies.

Perhaps one respondent framed it best: “Security is a nexus—it interacts, intertwines, and integrates with all” areas of technology and operations at an institution. The CISO and the CISO’s staff sit at this nexus. This is a large load to be shouldered by a single individual or a small unit. Furthermore, in addition to managing a broad scope of work and influence, the CISO must have a light touch, since nothing motivates people to do something faster than being told not to. Mitigating the risks of information technology requires that campus stakeholders be motivated to comply with institutional security policies, or at least lack motivation to not comply. Doing this requires the CISO to project information security leadership across campus, strongly but with a gentle touch.
Advice for Current CISOs

- Consider the appropriate scope of responsibility for your position. This should depend on the strategy for projecting information security leadership on campus: Should information security be integrated with the IT infrastructure and leadership, or should it be separate from IT and be projected from a higher leadership position at the institution?

- Consider the appropriate number of staff to accomplish information security work on campus. This should depend on your current and ideal scope of responsibility and institutional complexity.

- Develop a vision for the future of your role:
  - Do you have responsibility for all relevant areas of information security? Are there areas that should be under your scope of work or areas that you should divest of?
  - Is your line of reporting optimal? How might it be improved to benefit the institution?
  - Do you have sufficient resources, including staff? What critical value might you be able to add with more staff?

- Exert influence across the institution and via informal relationships to build information security capacity on campus according to these determinations and your institution’s strategic planning process. CISOs who can effectively exert influence across the institution may find this as or even more critical than their formal reporting line.

- Identify areas of information security in which you believe that your skills are not as strong as in other areas. Seek out information security training and certification options, as well as other professional development opportunities to strengthen your skills in these areas.

- Ensure that you are taking an enterprise-wide perspective to information security at your institution. Collaborate with other leaders across campus.

- Build external professional networks through associations including EDUCAUSE and peer-based organizations.
Advice for the CISO’s Supervisor

- Determine the appropriate job title for the CISO. While a job title is, to a certain extent, arbitrary, it is a signal to the institution and the profession about the position’s importance, its scope of work, and the nature of its responsibilities.

- Determine the appropriate reporting line for the CISO. This depends on the strategy that is most appropriate for the institution to project information security leadership on campus. Should this leadership flow from the campus IT unit or from higher up in the institutional hierarchy?

- Determine the appropriate size of the information security unit at the institution. This should depend on the CISO’s current—and ideal—scope of responsibility at the institution, as well as institutional complexity.

- Discuss with the CISO areas in which they feel the need for professional development. Provide time and resources for the CISO to pursue appropriate professional development opportunities, including training and certification options.

- When seeking to hire a CISO, look for candidates from both within and outside your institution. Look for individuals currently in information security–related positions, as well as in other positions that are technical in nature but not explicitly focused on information security.
Advice for Aspiring CISOs

- Gain experience in the major areas of CISOs’ scope of responsibility: developing policies and processes to address information security risks, maintaining the institution’s security infrastructure, managing information security incidents when they occur, and acquiring security systems and coordinating with vendors.

- Develop an understanding of the mechanisms for projecting information security leadership on campus by building partnerships across the institution.

- Develop an understanding of the mission and strategic direction of the institution and how information security can support them.

- Gain experience in as many of the essential roles an information security leader plays as possible, as well as in the skills necessary to fulfill those roles. Seek appropriate professional development opportunities, including professional certifications and volunteer opportunities.

- Advanced degrees are useful for gaining leadership skills and a broad perspective, while certifications are useful for gaining specific technical skills. Both are useful, and it is worthwhile earning both.

- Credibility is one of the skills CISOs rate as most important to their success. Credibility comes from both having an information security–related certification or other credential and from being in tune with the institution’s business operations and strategic direction.
Methodology

Survey invitations were sent to a pool of potential respondents with profiles in the EDUCAUSE member database indicating that they were CISOs or held an equivalent position, to active volunteers within the Higher Education Information Security Council, and to other CISOs identified by the respondents to the other ECAR studies of the IT leadership in higher education. A total of 101 senior CISO respondents completed the survey. Respondents were from 38 states spanning all regions of the U.S., as well as from Canada, Australia, and the United Kingdom. U.S. respondents made up 95% of the sample; non-U.S. respondents made up 5% of the sample. Data collection took place in May of 2016.

Acknowledgments

The authors would like to thank our ECAR colleagues Ben Shulman, Statistician, for programming the CISO survey and for his work cleaning and analyzing the data, and Kate Roesch, Data Visualization Specialist, for producing the graphics in this report. The contributions of our reviewers and subject-matter experts improved this report immensely: Susan Grajek, Vice President for Communities and Research, EDUCAUSE; Valerie Vogel, Senior Manager, Cybersecurity Program, EDUCAUSE; D. Christopher Brooks, Interim Director of Research, EDUCAUSE; Cathy Bates, higher education consultant and former CIO and CISO; and Sharon Pitt, Associate Vice President and CIO at Binghamton University.
Notes

1. We recognize that there are a variety of domains of security and that the terms “information security,” “IT security,” “cybersecurity,” and just plain “security” all refer to different sets of practices around different systems. This report concerns “information security,” and we try to use that term consistently throughout. If we use a different term, it is because we are citing a specific use of that term: mentioning a job title, quoting a respondent, or citing prior work that uses that term.


6. An important distinction must be made between “title” and “position.” A job title is what is on one’s business card: IT security officer, chief information security officer, etc. One’s position is more amorphous; it is one’s function and scope of responsibility. Different individuals with different job titles may be considered to have the same position—for example, an IT security officer and a chief information security officer.

7. This figure is considerably higher than that reported for Forbes Global 2000 companies, in which 40% of CISOs reported to the CIO in 2015. See Jody R. Westby, Governance of Cybersecurity: 2015 Report—How Boards & Senior Executives Are Managing Cyber Risks (Atlanta: Georgia Tech Information Security Center, October 2, 2015).

8. According to Jeffrey Pomerantz in IT Leadership in Higher Education, 2016: The Chief Information Officer, research report (Louisville, CO: ECAR, March 2017), 71% of respondents have the title chief information officer; most of the rest were split between two titles: vice president and director.


10. For our analyses we divided institutions into categories based on enrollment size (full-time equivalent). These categories were derived from Integrated Postsecondary Education Data System (IPEDS) data for fall 2014. The categories are as follows: very small (less than 2,000), small (2,000–3,999), medium (4,000–7,999), large (8,000–14,999), and very large (15,000+). Please note that the Carnegie Classification of Institutions of Higher Education uses these same categories of institutional enrollment size in the size and setting classification variable. However, our operationalization of size categories differs from Carnegie’s. For Carnegie, a very small two-year institution has fewer than 500 students, while a very small four-year has fewer than 1,000, for example. Our categories, however, are consistent across all institution types: small is small whether it’s a bachelor’s or a doctoral institution.

11. While very large doctoral institutions may indeed have the resources to support an entire department dedicated to information security, this particular institution is an extreme outlier: 2016 data from the Core Data Service show that central IT units at public doctoral institutions have 0.3 information security FTE per 1,000 institutional FTE. This particular institution has fully an order of magnitude more information security FTE than would be expected from this Core Data Service finding. See EDUCAUSE Almanac for Core Data Service, All Public Doctoral Institutions, March 2017.
12. To be fair, it is common for those reporting to the board to have their comments approved by their supervisor. In part this helps ensure that no report comes as a surprise; in addition, it simply helps manage the agenda for the board meeting.


14. The astute reader will note that many of the information security program areas mentioned in this section also align with industry information security standards such as those produced by the U.S. National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).


16. The percentage of time spent on various activities sums to 100% for each individual respondent. The medians presented here, however, are across all respondents and therefore do not sum to 100%.


22. See “Certified Information Security Manager,” ISACA.


25. The findings in this section are results of a re-analysis of data from Jeffrey Pomerantz and D. Christopher Brooks, *The Higher Education IT Workforce Landscape Report*, 2016, research report (Louisville, CO: ECAR, April 2016). For a more in-depth view of career trajectories within the higher education workforce, see the Career Paths: Higher Education IT Sectors interactive graphic.


29. The areas we asked about in our research are loosely based on the information security domain areas mentioned in the HEISC Information Security Guide: Effective Practices and Solutions for Higher Education. The guide is based on industry best practices and standards for the practice of information security.

30. Responses to these questions were on a Likert scale, ranging from *No experience; none needed* to *Expert-level experience; no more needed*.


32. Responses to these questions were on a Likert scale, ranging from *Not at all important* to *Extremely important*.

33. Responses to these questions were on a Likert scale, ranging from *Strongly disagree* to *Strongly agree*.

34. Responses to these questions were on a Likert scale, ranging from *Not at all important* to *Extremely important*.

35. Responses to these questions were on a Likert scale, ranging from *No expertise* to *Expert*.

36. See *Higher Education Information Security Council (HEISC) Charter*.

