2015 Higher Education
Chief Information Security Officer Study

By Wayne A. Brown, Ph.D.
Center for Higher Education
Chief Information Officers Studies, Inc.

Center for Higher Education Chief Information Officer Studies, Inc.
P.O. Box 38083
Albany, NY 12203
www.CHECS.org
© 2015 All rights reserved
2015 Sponsors

We are deeply grateful to our sponsors who support our higher education technology leadership research. Our sponsors have helped us expand from chief information officer studies to technology leadership and, now, to include chief information security officers. These sponsors believe this research is important, and they are as committed as we are to technology executive enrichment, growth, and education. We are pleased to present our generous sponsors who make this research possible.
We also want to acknowledge the higher education institutions who have sponsored CHECS through a site license purchase. Their contribution through this site license helps support our research and development efforts. It also signals the importance placed on this work by the very people who work in the field. If you would like your institution to become a sponsor, please consider purchasing a site license for one or more of the reports. The license grants your institution the right to share the report with all of its employees.
# TABLE OF CONTENTS

2015 Sponsors ................................................................................................................................. 2
2015 Institution Sponsors .................................................................................................................. 3
Acknowledgement ........................................................................................................................... 8
2015 CHECS Advisory Board ......................................................................................................... 10
Executive Summary ......................................................................................................................... 11

**INTRODUCTION** ......................................................................................................................... 14

**CHARACTERISTICS OF THE CISO** ............................................................................................ 15

- **Age** ........................................................................................................................................... 15
  - Age of CISOs, Figure 1 ........................................................................................................ 15
  - TL, CISO, and CIOs over 51 Years Old in 2015, Figure 2 .................................................. 15
- **Gender** .................................................................................................................................... 16
  - Gender, Figure 3 ................................................................................................................... 16
  - Percentage of Female CISOs, TLs, and CIOs in 2015, Figure 4 .......................................... 16
  - CISO Age and Gender, Figure 5 ........................................................................................... 17
- **Race** ........................................................................................................................................ 17
  - CISO Race, Figure 6 ............................................................................................................. 17
  - Percentage of Minority CISOs, TLs, and CIOs in 2015, Figure 7 ........................................ 18
  - Percentage of Hispanic CISOs, Figure 8 .............................................................................. 18
  - Percentage of Hispanic CISOs, TLs, and CIOs in 2015, Figure 9 ........................................ 19
- **Institution Types** ...................................................................................................................... 19
  - Institution Type Distribution, Figure 10 ............................................................................... 19
- **Tenure** .................................................................................................................................... 20
  - Tenure in Current Position for 2015, Table 1 ....................................................................... 20
- **Retirement Plans** ..................................................................................................................... 20
  - CISO Retirement Plans, Figure 11 ....................................................................................... 20
  - Projected Retirement in Next 10 Years (2015), Figure 12 ................................................... 21
  - CISO Retirement Plans by Gender, Figure 13 ...................................................................... 21
  - CISO Retirement Plans by Gender and Age, Table 2 ........................................................... 22
- **Previous Positions** .................................................................................................................. 23
  - Titles Held Prior to Current CISO Position, Table 3 ............................................................ 23
  - CISO Two Positions Prior Title, Table 4 .............................................................................. 24
  - CISO Sector for Last Position ................................................................................................. 24
  - CISO Sector for Their Last Position, Figure 14 .................................................................... 24
Acknowledgement

Many people are involved in the effort to produce this study, and two of the most important are the higher education chief information security officer (CISO) and the higher education chief information officer (CIO). In its second year collecting CISO data, CHECS has begun an effort for which it is known in the higher education CIO field, documenting the evolution of a career field. Certainly, gathering information from as large and varied of a population as every higher education CISO in the United States, can be challenging, and I am grateful to everyone who participated in the study. Without those individual responses, we would not have as full and as developed aggregate picture as we do of today’s higher education CISO. As a CIO, I know how busy everyone is and time is a valuable resource of which everyone is protective. That each of you invested your time into this study means you recognize its significance. I do not take your investment lightly, and your commitment and feedback motivates me to continue these studies. To each and every one of you, a sincere thank you.

I also want to specifically thank Tammy Clark, Cathy Hubbs, and Lanita Collette for their feedback on the CISO survey, direction of the research, and this very important position. It was invaluable to me to be able to work with them and hear their thoughts on this critical position.

CHECS’ sponsors, likewise, deserve accolades. I cannot express my gratitude enough to them. They are committed to the higher education technology profession and through their steadfast support, CHECS is able to not only continue its annual studies, we have expanded it. In 2014, we launched this study focusing on CISOs. We also introduced an exciting and well-attended Webinar series (checs.webex.com) that brought study results and respected guest panelists together for energetic and revealing discussions. Our Webinar topics ranged from study results to how to prepare for the executive technology role. If you have an opportunity, please thank our sponsors directly. They do not have the pleasure to speak with you about CHECS often, but they would like to know more about how their financial support impacted you.

Another significant group is the CHECS’ advisory board. The board has been very active and we could not have accomplished some of our efforts without their support. The all-volunteer board has devoted countless hours to the CHECS’ mission: Contributing to the education and development of the CIO in higher education. Our esteemed board of CIOs, CISOs, and technology leaders have generously shared ideas, experiences, and advice to advance the higher education technology leadership field. We enjoyed a phenomenal Webinar series with their inspiration and participation. With heartfelt gratitude, I applaud the CHECS advisory board.
As you may know, CHECS is an all-volunteer, nonprofit organization. We do not have a paid staff. Funds raised through report sales and resume services are reinvested directly into CHECS in support of its mission to the development of higher education technology professionals. To that end, we have endowed perpetual academic scholarships at several universities. The scholarships are aimed at technology students at different levels of education, from undergraduate to graduate to doctoral candidates. Each year, a $1,000 scholarship is awarded to a technology student in each program. The scholarships were created to recognize influential technology or education leaders who have left a lasting mark on CHECS. Through these scholarships, CHECS is helping future technology leaders who may become leaders within higher education. The scholarships are:

- **The Dr. Trudy Abramson Scholarship**, Nova Southeastern University, Fort Lauderdale, Florida - $1,000 scholarship to a doctoral student
- **The Dr. Polley Ann McClure Scholarship**, University of Texas, Austin - $1,000 scholarship for a female or minority undergraduate student
- **The Dr. Detlev H. Smaltz Scholarship**, Florida State University, Tallahassee, Florida - $1,000 scholarship to a graduate student
- **The Stephen Pribyl Scholarship Fund**, Excelsior College, Albany, New York (has not reached distribution threshold yet), need-based scholarship for women and minorities

We also want to thank Dr. Herb Smaltz. Our surveys for the chief information officer and institution management teams are based on his 1999 doctoral healthcare research. We are ever grateful to Dr. Smaltz for his permission to base our surveys on his survey.

The research, reports, scholarships, and Webinars are all efforts in line with CHECS’ mission. Our mission could not be achieved without your continued support. Thank you again.

Best regards,

Wayne A. Brown, Ph.D.
WBrown@CHECS.org
2015 CHECS Advisory Board

Keith McIntosh (Chair), Associate Vice President & CIO, Ithaca College

Jill Albin-Hill, Vice President and CIO, Dominican University

Pam Arroway, Senior Statistician, EDUCAUSE

Sharon Blanton, Vice President and CIO, The College of New Jersey

James Bradley, Former Vice President and CIO, University of Texas at Arlington

Curtis (Curt) Carver, Vice President and CIO, University of Alabama Birmingham

Jeffrey Cepull, Vice President for Information Resources and CIO, Philadelphia University

Tammy Clark, Chief Information Security Officer, University of Tampa

Lanita Collette, University Information Security Officer, Northern Arizona University

Stephen deFilipo, CIO, MSOE University, Milwaukee School of Engineering

Jay Dominick, Vice President and CIO, Princeton University

Maggie Fung, CIO, Kwantlen Polytechnic University

PB Garrett, Assoc. Provost & Chief Academic Technology Officer, The George Washington University

Joel Hartman, CIO, University of Central Florida

Cathy Hubbs, Chief Information Security Officer, American University

Ann Kovalchick, Associate Vice Chancellor and CIO, UC Merced

Susan Malisch, Vice President and CIO, Loyola University Chicago

Charlie Moran, Sr. Partner and CEO, Moran Technology Consulting

Joe Moreau, Vice Chancellor, Technology and CTO, Foothill-DeAnza Community College District

John (Jack) Suess, Vice President for IT and CIO, University of Maryland Baltimore County

Justin Sipher, Vice President of Libraries and IT, St. Lawrence University

Rhonda Spells, Interim Vice President for IT and CIO, Prince George’s Community College

Melissa Woo, Vice Provost for Information Services and CIO, University of Oregon
Executive Summary

The higher education chief information security officer (CISO) of 2015 is a complex position and the individuals holding the position are just as complex. The CISO has many of the same challenges that the higher education CIO of the 1990s had. In other ways, they have many of the same challenges of the higher education CIO of 2015.

The higher education CIO of the 1990s struggled for recognition of the importance of technology and the need to have their position recognized through title, placement on the executive team, and reporting to the President. The CIO of 2015 still struggles with two of these issues. The percentage of CIOs who sit at the executive table has been relatively steady, in the mid- to high-50 percent range, over the past 12 years. Likewise, the percentage of CIOs reporting to the President has remained steady over the same timeframe in the low- to mid- 30 percent range. Some part of the challenge that CIOs face is due to the fact that the institution management team (IMT) members (other vice presidents and the president) don’t understand the CIO job and believe that it is a very technical position. The importance of this observation is found in the fact that in most cases, the CIO reports to an IMT member and the IMT members are writing the job description and involved in the CIO hiring process. The CISO faces a similar challenge because they primarily report to the CIO or someone who reports to the CIO and the CIO may not understand the CISO job or the skills required to do it. This challenge is compounded when you consider that the CIO is ultimately responsible for hiring the vast majority of CISOs.

CHECS research has found that an advanced degree is a CIO requirement according to the CIO and IMT. In addition, the minimum education requirement for higher education executive positions tends to be an advanced degree. Likewise, if the CISO hopes to join the CIO at the executive table, this education requirement is sure to be placed on them. Unfortunately, of the three groups, the CIO, TL, and CISO, the CISO is the least likely to hold an advanced degree. There were 58 percent of the CISOs who had an advanced degree. The percentage is significantly less than the CIOs and TLs. However, only 51 percent of the CISOs believed an advanced degree was required for a CISO and for the CIOs this CISO education preference was even less at 42 percent. The majority of CIOs in the CISO research indicated the CISO should have a technology major and in fact, 39 percent of them did have a technology major.

Less than fifty percent of the CISOs were over 51 years old and of the three groups, CISOs, CIO, and TLs, they are the youngest. Only 15 percent of the CISOs were female compared to 25 percent of the CIOs and 31 percent of the TLs. Nine percent of the CISOs were minorities, which was the most diverse of the CIOs, TLs, and CISOs.

The majority of CISOs followed a career path that took them through very traditional roles in an information technology (IT) department. The typical CISO has not spent as much time in his or her current position as the CIO or TL. However, the CISO retirement plans only has 25 percent of them planning on retirement in the next ten years.

Over 40 percent of the CISOs arrived at their current position from outside of higher education. There were 17 percent more of the CIOs who had last worked in higher education. Perhaps this difference in CISO last sector is due to higher education being late to the importance of information
security or it could be that junior information security professionals are leaving industry to advance their careers in higher education. Just over 50 percent of the CISOs were internal candidates for their current position and 43 percent of the CISOs said the term “chief” was in their title.

The CIOs and CISOs were asked to select the five most important skills for a CISO. The CIOs chose four IT-focused skills and communication. The CISOs selected three soft skills, communication, leadership, and interpersonal skills along with two technical skills. The literature on the CISO indicated soft skills are needed for the position. However, the CIO, who supervised the vast majority of CISOs may be hiring based on their CISO technology-focused view of skills. This CISO-skill difference of opinion will contribute to the disparity between the literature-cited skills and actual CISO skills. Furthermore, CISOs who lack soft skills may not be able to effectively operate as members of the institution management team (IMT) or reporting to the chief executive officer (CEO).

There has been a great deal of debate about where a CISO should report in the organization hierarchy and whether or not the CISO should serve on the institution management team (IMT). Seven percent of CISOs said they reported to the President while 77 percent reported to the CIO and another nine percent reported to someone who reported to the CIO. The CISO ideal reporting configuration for 36 percent of the CISOs was reporting to the President. Another 42 percent of CISOs indicated they should report to the CIO. The majority of CISOs interacted formally with the President once a year or less. The CIO reality and opinion on ideal CISO reporting were closely aligned with 74 percent of the CIOs indicating that the CISO reported to them. Seventy five percent of the CIOs thought the CISO should report to the CIO. Only 23 percent of the CISOs served on the IMT and 35 percent of the CISOs reported monthly interaction with the IMT. In the CHECS CIO research, 57 percent of the CIOs were IMT members.

The CIOs and CISOs were asked to recommend activities to prepare someone to become a CISO. The four most frequently selected activities were the same for the CIO and CISO. The activities were professional development, mentoring, on-the-job training (OJT) and certifications. This preparation activity approach differed from CIO preparation where mentoring and OJT were the preferred methods. Perhaps, the existence of a formal body of knowledge for information security had some impact on this difference.

The majority of CISOs used NIST and SANS as their security models and over 60 percent of CISOs found their model to be valuable. Disturbingly, only 13 percent of CISOs considered their security program to be mature or a leader. CIOs agreed with the CISO assessment with only 10 percent of the CIOs considering their security program to be mature or a leader. Perhaps not surprisingly, the CIOs who was also the CISO had the lowest percentage, six percent, who viewed their program as mature or a leader. Program maturity may be effected by the resources devoted to the program. There were 38 percent of the CISOs and 57 percent of the CIOs who indicated there was not a dedicated security budget while this same answer accounted for 75 percent of the CIOs who were also CISOs. Almost a third of CISOs and one fifth of the CIOs had experienced a disruption in critical IT services in the past three years while almost half of the CISOs and a third of the CIOs had experienced a data breach. Considering the high profile nature of a breach and the potential cost, it would make sense for organization to have the best person leading the information
security programs, fund it well and provide the staffing to ensure its success ("Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," 2014). There was some agreement between CIOs and CISOs about the priority order and importance of the CISO roles but the CIOs considered four of the six CISO roles as less than effective.
INTRODUCTION

The chief information security officer (CISO) is a relatively new role in higher education just as the chief information officer role was new in the mid-1990s. ECAR reported on the information technology security officer in 2009 (Goodyear, Salaway, Nelson, Petersen, & Portillo, 2009). The CISO role has steadily evolved as the information security threats have increased. While the position has risen through the IT department, its importance may be driving the need for a CISO with strategic focus (Brenner, 2010; Slater, 2005). Indeed, IBM reported there was a drive to expand CISOs’ responsibility so it was not just a defensive position (van Zadelhoff, Lovejoy, & Jarvis, 2013). In this second year of the CHECS CISO research, it became clear that there was a difference of opinion between the CIO and the CISOs about which skills are required to be a CISO. The CISOs focus on soft skills while the CIOs indicate it is a position that requires more technical skills. It is interesting to note the CIOs in the CHECS research encounter the same challenge in that the institution management teams (IMT) believe the CIO should be a technology-focused position.

In July 2015, higher education CISOs and CIOs were invited to participate in a CHECS CISO survey. Both surveys contained some identical questions to gather data from different perspectives. Thirty-seven percent of the CIOs who participated in the survey indicated they also served as the CISO. Data collected from this group of CIO/CISO are presented separately for some subjects. In addition, results from the CHECS 2015 CIO and Technology Leader research are also presented as a comparison to the CISO (Brown, 2015a, 2015b).

This report is divided into three sections. The first section examined CISO characteristics. The second section reviewed the security programs at institutions, and the final section reported on the importance of CISO roles and their effectiveness operating in those roles based on CISO and CIO assessments.
CHARACTERISTICS OF THE CISO

Age

The higher education CISOs were a younger group than the higher education CIOs in the CHECS research. As in 2014, the majority of the CISOs, 56 percent, were under 51 years.

Age of CISOs, Figure 1

![Figure 1](image)

More than half of all 2014 CISOs are under 51 years old.

While a majority of CISOs were younger than 51 years, the average higher education CIO was older than 51 years old. In fact, the percentage of CIOs who were 51 years or older continued to rise and reached 69 percent in 2015. In the technology leader (TL) research, 46 percent of the TLs were 51 years old or older. The following charts reflects the percentage of those who were 51 years old or older in the three technology professions.

TL, CISO, and CIOs over 51 Years Old in 2015, Figure 2

![Figure 2](image)

Based on percentages, there were significantly more CIOs who are 51 years or older than TLs or CISOs.
Gender

Over the life of the CHECS research, there have been gender disparities in the CIO and TL populations with women making up a small percentage of the population. Indeed, the CISO research reflected this same disparity with women making up only 15 percent of the respondents. This lack of gender diversity among CISOs may be a reflection of a career path through a historically male-dominated information technology (IT) department. This disparity is even more pronounced when you consider that in 2015, more than 56 percent of higher education students were women (Almanac Issue 2015-2016, 2015).

Gender, Figure 3

The percentage of female CIOs rose to 25 percent in 2015 (see the below figure). For the TL profession, the percentage of female TLs was more than double that of the CISOs, but the TL percentage was a decline from the 2014 high of 39 percent. The drop in the female TL percentage may be a red flag for the future because this population is the conduit for the CIO position, and, in due time, it may have a negative impact on the overall percentage of female CIOs.

Percentage of Female CISOs, TLs, and CIOs in 2015, Figure 4

Figure 3 The CISO profession in higher education is overwhelming dominated by men.

Figure 4 2015 Female CISOs, TLs and CIOs
In some cases, studying populations by age groups and gender can highlight significant differences. In the case of the higher education CISO, the data revealed almost half of the female CISOs (45 percent) were in one age group: the 41-45 age bracket (see the figure below). Another 45 percent of female CISOs were in two groups, comprising those aged from 56 to 65 years old, while there was zero percent in the 46-50 and the 51-55 age groups. In comparison, male CISOs were more evenly distributed across the age ranges. However, as with the female CISO group, the three largest male CISO age group percentages were in the same ranges as the female CISOs.

**CISO Age and Gender, Figure 5**

![CISO Age and Gender](image)

**Race**

In CHECS studies, higher education CIOs and TLs have not been racially diverse. Likewise, in CHECS’ 2015 study, the higher education CISOs were also not diverse. Eighty-six percent of the CISOs were White. Nine percent were evenly divided at three percent each for American Indian or Alaska Native, Asian, and Black or African American; nine percent declined to respond (see Figure 6 below). As a comparison, in 2015, 53 percent of higher education enrollments and 74 percent of the U.S. population were White (*Almanac Issue 2015-2016*, 2015).

**CISO Race, Figure 6**

![CISO Race](image)
The 2015 percentage of minorities holding the CISO, TL, and CIO positions are compared below. The low percentages of minorities in these roles continue to not be reflective of the population higher education serves.

**Percentage of Minority CISOs, TLs, and CIOs in 2015, Figure 7**

![Bar chart showing percentages of CISOs, TLs, and CIOs by minority status.](chart)

*Figure 7 Among the CIO, TL and CISO groups, less than 10 percent of respondents were minorities. The least percentage was reported in the TL group with only 5 percent.*

The percentage of Hispanic CISOs is depicted in Figure 8. Five percent of the CISOs reported they were Hispanic. Another seven percent declined to answer. The percentage of higher education students in the United States who were Hispanic was more than 14 percent in 2015 (*Almanac Issue 2015-2016*, 2015).

**Percentage of Hispanic CISOs, Figure 8**

![Pie chart showing percentage of Hispanic CISOs.](chart)

*Figure 8 Five percent of respondents reported they were Hispanic, while another seven percent declined to respond. The percentage of Hispanic CISOs is in sharp contrast to 88 percent who reported they were White.*
While the percentage of Hispanic CISOs was below 10 percent, it was a greater percentage than either CIOs or TLs. The results are presented in Figure 9.

**Percentage of Hispanic CISOs, TLs, and CIOs in 2015, Figure 9**

![Figure 9 Combined only 5 percent of CIOs and TLs reported they were Hispanic compared to five percent of CISOs.](image)

**Institution Types**

The CISO in higher education is a relatively new position. Although many CIOs continue to be responsible for technology security, as cyber threats become more prevalent, institutions are creating a designated security officer position separate from the CIO position. Nevertheless, the CISO position may not be found in every institution or in large numbers among every institution type. As a result, in this research, the represented organizations in this study did not reflect the overall makeup of U.S. institutions. For example, this study had a majority of responses (65 percent) from doctorate level institutions while, according to the *Chronicle of Higher Education* in 2012 only six percent of institutions were doctorate. The following chart illustrates the higher education institution types in the United States according to the *Chronicle of Higher Education* and the responding CISOs (*Almanac Issue 2012-2013*, 2012).

**Institution Type Distribution, Figure 10**

![Figure 10 While doctorate type institutions represent the least percentage nationwide, they were the highest responding group in the CISO study, making them the highest represented.](image)
Tenure

The CIO tenure declined in 2015 to five years and nine months, the second lowest level since 2003. The TLs enjoyed the longest tenure of the three groups at six years and five months. Survey results indicated the average tenure for CISOs in their current position was five years and three months. The results for the three groups are depicted in the following table.

Tenure in Current Position for 2015, Table 1

<table>
<thead>
<tr>
<th></th>
<th>CISO</th>
<th>TL</th>
<th>CIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Years</td>
<td>5</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Months</td>
<td>3</td>
<td>5</td>
<td>9</td>
</tr>
</tbody>
</table>

*Table 1 On average, TLs had the longest tenure in 2015, 8 months longer than CIOs and more than a year longer than CISOs.*

Retirement Plans

Almost 50 percent of the higher education CIO population has consistently predicted their retirement in the next 10 years. The CISOs, however, are a younger group than the CIOs and it is reflected in their retirement plans. Only 25 percent of the CISOs predicted retirement in the next decade. The CISO retirement predictions are illustrated in the following chart.

CISO Retirement Plans, Figure 11

*Figure 11 More than half of responding CISOs do not plan to retire for at least another 16 years, at the earliest, and nearly a third plan to continue working for two more decades.*

A comparison for the projected retirement for CISOs, TLs, and CIOs in the next 10 years is depicted in Figure 12. A greater percentage of CIOs and TLs, over CISOs, expect to retire.
Projected Retirement in Next 10 Years (2015), Figure 12

Among the three groups (CIOs, TLs, and CISOs), CISOs were the smallest percentage in the projected plans to retire within the next 10 years.

The retirement plans of the male and female CISOs were relatively consistent in a gender comparison. In the next decade, 27 percent of the female CISOs plan to retire versus 26 percent of the male CISOs (Figure 13).

CISO Retirement Plans by Gender, Figure 13

Overall, there was little difference in the retirement plans for men and women holding the CISO position.
The following table depicts the CISO retirement plans by age groups and gender. A comparison between the genders is difficult because all of the female CISOs were represented in four age groups: 36-40, 41-45, 56-60, and 61-65, while men were represented in age groups from 26 years up to 70 years old.

When confining the analysis to the age groups where women were represented, there were some differences between the genders. For instance, 100 percent of the women between the age of 36 and 40 were predicting they would retire within the next 16 to 20 years, while only 22 percent of the men in that same age range had the same retirement plans. In the 56 to 60 age range, more male CISOs (77 percent) predicted retirement in the next 10 years compared to 33 percent of female CISOs.

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Female</th>
<th>Male</th>
</tr>
</thead>
<tbody>
<tr>
<td>21-25</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>26-30</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>31-35</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>36-40</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>41-45</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>46-50</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>51-55</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>56-60</td>
<td>33%</td>
<td>0%</td>
</tr>
<tr>
<td>61-65</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>66-70</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>71 and older</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

The table shows that women were represented in only four age brackets whereas men were represented in almost every age bracket, except the youngest and oldest groups.
Previous Positions

As with the higher education CIO position, the career path for the CISO has been varied and can be confusing to those striving to reach the role. One way to help clarify the career path is to examine the course taken by current CISOs. CISOs provided the job titles for their last two positions prior to taking on the senior information security role. By examining these previous positions, a career path may begin to take shape for the CISO role.

The following table lists the position held by CISOs prior to their current post. Thirty-five percent of the respondents held the CISO or senior security position in their last job. Twenty-three percent of CISOs reported they held either the Systems or Network Director (or Manager) position and nine percent held an Executive Director role within the IT department. As may be expected, 83 percent of current CISOs held specific roles considered to be traditional IT department positions. Only 1 percent did not work in IT.

<table>
<thead>
<tr>
<th>Titles Held Prior to Current CISO Position, Table 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO or senior IT security position</td>
</tr>
<tr>
<td>Systems Director/Manager</td>
</tr>
<tr>
<td>Network Director/Manager</td>
</tr>
<tr>
<td>Executive Director</td>
</tr>
<tr>
<td>Other</td>
</tr>
<tr>
<td>Information Security</td>
</tr>
<tr>
<td>Administrative Technology Director/Manager</td>
</tr>
<tr>
<td>Auditor</td>
</tr>
<tr>
<td>Application Development Director/Manager</td>
</tr>
<tr>
<td>Consultant</td>
</tr>
<tr>
<td>Did not work in the IT Department</td>
</tr>
<tr>
<td>Desktop Support Director/Manager</td>
</tr>
<tr>
<td>Academic Technology Director/Manager</td>
</tr>
</tbody>
</table>

This second table lists the job titles CISOs held two positions prior to their current post. This list is more varied than the list above. As with the previous list, many CISOs held a management position in the IT department. Sixteen percent of CISOs stated they held a systems director or manager position (see Table 4), while another 12 percent held the senior security position or CISO title. Another 9 percent worked in Information Security while seven percent held a network director/manager or analyst position. Seventy one percent of the CISOs worked in a traditional IT department two positions prior to their current security leader role. Clearly, the path to become a CISO has been carved through the technology department.
CISO Two Positions Prior Title, Table 4

<table>
<thead>
<tr>
<th>Position</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Director/Manager</td>
<td>16%</td>
</tr>
<tr>
<td>CISO or senior IT security position</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>9%</td>
</tr>
<tr>
<td>Information Security</td>
<td>9%</td>
</tr>
<tr>
<td>Network Director/Manager/Analyst</td>
<td>7%</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>7%</td>
</tr>
<tr>
<td>Executive Director of IT</td>
<td>5%</td>
</tr>
<tr>
<td>Application Development Director/Manager</td>
<td>5%</td>
</tr>
<tr>
<td>Auditor</td>
<td>5%</td>
</tr>
<tr>
<td>Consultant</td>
<td>4%</td>
</tr>
<tr>
<td>Didn't work in the IT Department</td>
<td>3%</td>
</tr>
<tr>
<td>Administrative Technology Director/Manager</td>
<td>3%</td>
</tr>
<tr>
<td>Academic Technology Director/Manager</td>
<td>3%</td>
</tr>
<tr>
<td>Military</td>
<td>3%</td>
</tr>
<tr>
<td>Faculty</td>
<td>1%</td>
</tr>
<tr>
<td>Desktop Support Director/Manager</td>
<td>1%</td>
</tr>
<tr>
<td>Help Desk Director/Manager</td>
<td>1%</td>
</tr>
<tr>
<td>Telecommunications Director/Manager</td>
<td>1%</td>
</tr>
<tr>
<td>Project Management</td>
<td>1%</td>
</tr>
</tbody>
</table>

Table 4 2015 CISOs reported the job titles for the roles they held two positions prior to their current CISO role.

CISO Sector for Last Position

To more clearly understand the path current CISOs took to arrive at their post, they provided information about the sector they worked in for their last position. A choice of five sectors was provided: Higher Education, Public (local, state, or federal government), Healthcare, Commercial or for profit, and Nonprofit outside of higher education. Figure 14 depicts the responses by sector. The majority of CISOs, 59 percent, came from Higher education. Another 24 percent were in the Commercial/for profit sector. The other three sectors collectively accounted for 17 percent of the CISOs.

CISO Sector for Their Last Position, Figure 14
In the CHECS CIO research, the higher education CIOs also provided information regarding their last position sector. The following chart compares the sectors CIOs and CISOs migrated from to their present position. Seventeen percent more of the CIOs had served in the Higher Education sector than CISOs, while nine percent fewer CIOs had served in the Commercial sector.

CISO and CIO Sector for Their Last Position, Figure 15

Figure 15 Overall, a greater percentage of CISOs, compared to CIOs, came from sectors other than Higher Education.

Figure 16 illustrates several CISO comparisons grouped by the five sectors. Since the number of survey respondents from the Public, Healthcare, and Nonprofit outside higher education were minimal, this section focuses only on the data from the Higher Education and Commercial sectors.
The greatest differences between the *Higher Education* sector CISOs and those from the *Commercial* sector were surprising when comparing the results to CHECS’ CIO research findings. For example, 21 percent of CISOs from the *Commercial* sector were women compared to 11 percent from *Higher Education*. In the CIO research, less of the *Commercial* sector CIOs were women. Moreover, 54 percent of CISOs from the *Commercial* sector held an advanced degree compared to 45 percent of CISOs from *Higher Education*. In the CIO research more of the *Higher Education* CIOs held an advanced degree compared to the *Commercial* sector.

Seven percent of the *Higher Education* CISOs reported to the CEO while five percent of those from the *Commercial* sector had that reporting relationship. Thirty-two percent of the *Commercial* sector CISOs served on the Institution Management Team (IMT) compared to 23 percent of the *Higher Education* sector CISOs.

**CISO Last Position Sector Comparison, Figure 16**

*Figure 16 A higher percentage of Commercial sector CISOs compared to those from Higher Education served on the institution management team and held an advanced degree.*
CISO Internal Candidates for Current Position

In some circles, there is a debate about whether or not an internal candidate can be competitive for a senior technology position. In the CHECS CIO research, a significant percentage of the CIOs, 42 percent, were employed by their current institution prior to being selected for the CIO position. In 2015, 51 percent of the CISOs indicated they were employed by their current institution before assuming the CISO title (Figure 17).

CISO Position as an Internal Hire, Figure 17

![Pie chart showing 51% Yes and 49% No for CISOs being internal candidates.]

Figure 17 Slightly more than half of 2015 CISOs were employed by the same institution prior to being selected as the CISO.

The following chart illustrates a comparison between 2015 CIOs and CISOs who were internal candidates for their current positions. A higher percentage of CISOs were selected from within the institution for the information security leader role.

Internal Candidates 2015, Figure 18

![Bar chart showing 42% CIO and 51% CISO for internal candidates.]

Figure 18 A small percentage of institutions hired a CIO from within their organization in comparison to CISOs.
The following Figure depicts a comparison for CISOs who were internal and external candidates for their current posts. The Figure provides a comparison for *gender, those older than 51 years, retirement plans, advanced degree, reporting to the CEO, and IMT membership*. There were only two areas where there was a difference of 10 percent or more. There were more of the internal candidates—34 percent—predicting retirement in the next decade compared to 16 percent of the external candidates. Seventy-six percent of the external candidates had an advanced degree versus 42 percent of the internal candidates. This advanced degree difference might indicate that candidates for the CISO position with an advanced degree have an advantage over those who do not have an advanced degree.

**Internal/External CISO Comparison, Figure 19**

![Bar chart comparing internal and external CISO candidates on various attributes.](image)

*Figure 19* Among most of the comparisons, there was little difference between the internal and external CISO candidates. Differences were the most notable regarding retirement plans and advanced degree holders.

**Current CISO Titles**

Titles can be important as it might indicate the importance an organization places on a function. Indeed, the higher education CIO community struggled for a number of years to be recognized as the “chief” information officer. The CISO career field may also be facing a title struggle. Their titles are shown in the following Figure. CISO was the most frequently listed with 43 percent of the respondents holding that title. However, another 20 percent reported holding the Director title.
Current Title of CISOs, Figure 20

Figure 20 Fifty-six percent of CISOs reported holding a title other than “Chief Information Security Officer.”

Degree Level

In higher education, key executives are expected to have an advanced degree. In the CHECS CIO and TL research, two-thirds or more of the survey respondents held an advanced degree. Moreover, the IMT respondents almost unanimously indicated an advanced degree requirement for the CIO position. In 2015, 58 percent of CISOs held an advanced degree.

Degree Level for CISO, Figure 21

Figure 21 More than half of CISOs held an advanced degree.
Figure 22 depicts an advanced degree comparison for CISOs, CIOs and TLs for 2015. The CISOs had the smallest percentage among the three groups. The percentage of TLs with an advanced degree has steadily increased since CHECS began collecting degree-held data in 2009. CIOs with an advanced degree has been relatively steady since 2003, when CHECS research began.

**Advanced Degree for CISO, CIO and TL, Figure 22**

![Figure 22](image)

*Figure 22 Only 58 percent of CISOs have an advanced degree, less than CIOs and TLs. The percentage difference may reflect the evolving CISO career field as institutions and professionals seek the appropriate education and requirements for the position.*

The CISOs and CIOs provided their opinions about what degree was necessary for the CISO position. The following two Figures reflect the two groups’ responses. Fifty-one percent of the CISOs indicated an advanced degree should be required. The full breakdown of CISO responses is illustrated in Figure 23.

**CISOs: Degree Required for the CISO, Figure 23**

![Figure 23](image)

*Figure 23 CISOs provided their opinion regarding what degree should be required for the CISO position.*
CIOs also voiced an opinion about the degree requirement for the CISO role. Less than half of the CIOs (42 percent) indicated that CISOs should have an advanced degree, while 55 percent believed a bachelor’s degree was sufficient. The CIOs’ degree expectations may have an impact on future CISOs as a large percentage of them currently report to the CIO.

**Degree Required for the CISO, Figure 24**

![Pie chart showing degree requirements for CISOs.](image)

*Figure 24 The majority of CIOs—97 percent—believe a CISO should have either a bachelor's degree or master's degree. None of them think a doctorate is necessary.*

The following chart provides a side-by-side comparison of the CIO and CISO responses regarding what degree was necessary for the CISO position. Part of the challenge for some CISOs in higher education is they may believe it is important to be a part of the IMT and to also report to the President. However, being an IMT member and reporting to the Chief Executive Officer (CEO), may, likewise, come with higher expectations for the CISO in terms of the degree held. In 2015, 90 percent of the IMT members expected CIOs to have an advanced degree. In the future, these IMT expectations for the CIO may become an obstacle for CISOs.

**Required CISO Degree Comparison, Figure 125**

![Bar chart comparing degree requirements between CIOs and CISOs.](image)

*Figure 25 CISOs and CIOs, alike, believe CISOs should have either a bachelor's or a master's degree.*
Degree Major

In addition to the degree level, the CISO degree major was also examined. Participating CISOs named their degree major, and as might be expected, Technology (39 percent) was the most frequently selected degree (Figure 26). As was found in CHECS’ TL and CIO research, there were a number of other degree majors represented. In the 2015 CIO and TL research, five majors represented 76 percent of the responses: Business, Technology, Education, Administration, Leadership, and Management. For the CISO, these majors combined accounted for 75 percent of the total responses.

The technology major is a natural selection for the CISO who, according to this research, has risen through the technology department ranks. However, in the CIO and TL research, the Technology major was not the dominating degree major. In fact, only 26 percent of CIOs and 25 percent of TLs held a Technology major. The following Figure depicts the percentage of CISOs, TLs, and CIOs who had a Technology major in 2015.

![Figure 26 Seventy-five percent of 2015 CISOs held a Technology or Business degree.](image)
Technology Major Comparison, Figure 27

Figure 27 In 2015, a greater percentage of CISOs held a Technology major compared to CIOs and TLs.

CISO Degree Major Opinions

CISOs expressed their opinion about the degree major a CISO should possess. The single largest response, 41 percent, was the *Degree was not important*. This response was followed by *Technology* at 35 percent. Figure 28 depicts the CISOs’ opinion regarding what major is important for the career field.
CISOs gave the same top two responses as the CISOs except in reverse order. More than 50 percent of the CIOs indicated a CISO should have a Technology major (Figure 29). Another 34 percent stated the major was not important. This CIO preference for a technology-focused CISO also revealed itself in the skills preference discussed in the next section of this report. In the CIO research, the CIOs most common degree major selection has been that the major was not important.

CIOs: Degree Major Needed for CISO, Figure 29
Figure 29 More than half of CIOs believed CISOs should have a Technology major.

Figure 30 depicts the contrast between the CIO and CISO opinion regarding the two most frequently named degree majors these groups listed as needed for the CISO position: Technology and Major not important. Eighty-eight percent of the CIOs selected one of these two degree majors compared to 76 percent of the CISOs.

Two Most Frequent Degree Majors Needed for CISO, Figure 30

Figure 30 CIOs did not believe a Technology major was as important for the CISO position as the CISO group believed.
Skills Needed by the CISO

Over the past 10 years, there has been some research and discussion about the responsibilities of a CISO which may help define the skills needed for the position. Cho (2003) highlighted skills and responsibilities that included communication, coordination, policy development, response to security threats, vendor selection and management, and the ability to evaluate risk versus business need. IBM later added vision, strategy, relationship building, policy, and risk management to the list (van Zadelhoff et al., 2013).

The CIOs in this research provided their insight regarding necessary CISO skills. The CIOs were presented with a number of possible CISO skills and asked to select five skills. They could select choices from the list or provide other skills that were not listed. The skills list and the percentage of CIOs who selected them are displayed in Table 5.

The 2015 list of CISO skills, according to the CIO, are primarily IT-focused with one soft skill, communication, at 61 percent. CIOs viewed the CISO as technology and policy-focused. The most frequently selected skill was IT security best practices knowledge at 81 percent. Technical knowledge, IT legal and policy expertise, and IT forensics were third, fourth, and fifth most frequently selected skills.

Gartner noted the CISO is expected to act as a “translator” for the functional areas and information security (Scholtz, 2013c). The communication expectation is one that is also applied to higher education CIOs. CHECS’ CIO research has found in the past that one of the two most important skills for the CIO has been communication.

In other research, the CISO has been viewed by executives as primarily technology focused (Vijayan 2014). On the other hand, Gartner found that executive skills were required for the CISO (Scholtz, 2013c). Scholtz (2013c) also reported that CISOs should have an understanding of the business of the organization. Again, this expectation has also been a finding for CIOs. Only 15 percent of the CIOs in this research selected Business knowledge as a skill needed by the CISO.

CIOs: Skills Needed by CISO, Table 15

<table>
<thead>
<tr>
<th>Skill</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Best Practices Knowledge</td>
<td>81%</td>
</tr>
<tr>
<td>Communication Skills</td>
<td>61%</td>
</tr>
<tr>
<td>Technical Knowledge</td>
<td>53%</td>
</tr>
<tr>
<td>IT Legal and Policy Expertise</td>
<td>39%</td>
</tr>
<tr>
<td>IT Forensics</td>
<td>38%</td>
</tr>
<tr>
<td>Computer Networks</td>
<td>35%</td>
</tr>
<tr>
<td>Leadership</td>
<td>32%</td>
</tr>
<tr>
<td>Interpersonal Skills (effective social interaction)</td>
<td>29%</td>
</tr>
<tr>
<td>Technology Governance</td>
<td>21%</td>
</tr>
<tr>
<td>Higher Education Knowledge</td>
<td>19%</td>
</tr>
<tr>
<td>Change Management</td>
<td>17%</td>
</tr>
<tr>
<td>Relationship Building</td>
<td>17%</td>
</tr>
<tr>
<td>Business Knowledge</td>
<td>15%</td>
</tr>
</tbody>
</table>
CISOs also provided their opinion regarding important skills for the position. As with the CIOs, they selected the five most important skills. Their results are shown in Table 6. Unlike CIOs, a majority of CISOs named Communication as most important followed by Leadership—these two skills were named the most important CIO skills, by CIOs, in the 2015 CHECS CIO research. IT Security Best Practices was the third most frequently selected skill followed by Interpersonal Skills and Technical Knowledge. The following Table depicts the CISO responses and it also shows the top five CIO-ranked responses for CISO skills.

### CISOs: Skills Needed by CISO, Table 6

<table>
<thead>
<tr>
<th>Skill Needed by CISO</th>
<th>CISO Response</th>
<th>CIO Response Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Skills (writing, listening, speaking)</td>
<td>84%</td>
<td>2</td>
</tr>
<tr>
<td>Leadership</td>
<td>72%</td>
<td></td>
</tr>
<tr>
<td>IT Security Best Practices Knowledge</td>
<td>68%</td>
<td>1</td>
</tr>
<tr>
<td>Interpersonal Skills (effective social interaction)</td>
<td>45%</td>
<td></td>
</tr>
<tr>
<td>Technical Knowledge</td>
<td>39%</td>
<td>3</td>
</tr>
<tr>
<td>Business Knowledge</td>
<td>38%</td>
<td></td>
</tr>
<tr>
<td>IT Legal and Policy Expertise</td>
<td>38%</td>
<td>4</td>
</tr>
<tr>
<td>Relationship Building</td>
<td>27%</td>
<td></td>
</tr>
<tr>
<td>Higher Education Knowledge</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>Technology Governance</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>11%</td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Computer Networks</td>
<td>7%</td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td>7%</td>
<td></td>
</tr>
<tr>
<td>Academic Computing Experience</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>IT Forensics</td>
<td>4%</td>
<td>5</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>Vendor Management</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>Administrative Computing Experience</td>
<td>3%</td>
<td></td>
</tr>
<tr>
<td>Supervision</td>
<td>1%</td>
<td></td>
</tr>
</tbody>
</table>
Table 6 2015 CISOs believe the position needs Leadership and Interpersonal skills, while CIOs believe CISOs are better served having Technical knowledge, IT Legal and Policy Expertise, and IT Forensic skills.

The following Figure shows a comparison between the CISO’s five most frequently selected skills and CIO selection of those same CISO skills. The CIOs’ three most frequently named skills were also selected by the CISOs among their top five skills chosen, but they were positioned in a different order based on the percentage of CISOs choosing that particular skill. CIOs favored technology skills while the CISOs leaned towards soft skills. The CISOs’ skills selections were more in line, than CIOs were, with other CISO research.

CISO Five Most Frequently Selected Skills for CISO Position, Figure 31

![Bar chart showing comparison between CISO and CIO skills selections.]

Figure 31 When examining skills needed for the role, CISOs placed more emphasis on soft skills than on technical skills in comparison to the CIO point of view.

Actual and Ideal CISO Reporting

Reporting to the CEO of an organization is a preference for many executives. Indeed, this reporting relationship is commonly expressed as a needed configuration due to the importance of the executive’s area of responsibility. Therefore, it is no surprise to find this same assertion on the CEO-reporting relationship in an area such as information security. The percentage of higher education CIOs reporting to the CEO has remained steady in the low 30 percent range since 2003.

As depicted in Figure 32, only five percent of the CISOs reported to the CEO in 2015. In the past, Gartner has reported the importance of CISOs being recognized and their reporting relationship being elevated to the CIO or similar level outside IT (Scholtz, 2013b). A total of 35 percent of CISOs reported within one level of the CEO.

CISO Reporting – Number of levels from CEO, Figure 32
The CISOs in this study provided their actual reporting configuration as well as their ideal configuration. As in 2014, the vast majority of CISOs, 77 percent, reported to the CIO (Figure 33). The percentage of CISOs reporting outside the IT department was slightly more than 10 percent.

The CISO ideal reporting configuration provided a view of their aspiration for this key role. Only 42 percent of CISOs believed directly reporting to the CIO was the ideal relationship. Another 36 percent indicated they should report to the institution president. The remaining responses were small and distributed over different reporting arrangements.

**CISO Reporting Title – Actual and Ideal According to CISO, Figure 33**
This study collected data to compare actual reporting structure against CISOs’ ideal structure. While a majority reported to the CIO, less than half believed that structure was ideal.

To provide a contrast, CIOs also provided actual and ideal reporting structure regarding the CISO role. Their responses are depicted in below in Figure 34. Seventy-four percent of the CIOs indicated the CISO reported to them. Moreover, 75 percent of CIOs believed this structure was the ideal reporting relationship. Another 18 percent of the CIOs indicated the CISO was one reporting layer away, reporting to someone who was supervised by the CIO. Only two percent of the CIOs indicated the CISO reported to the institution president and five percent of the CIOs believed that ideally the CISO should report to the president.
CISO Reporting Title – Actual and Ideal According to CIO, Figure 34

Figure 34 Three quarters of the CIOs believe CISOs should report the CIO compared to 5 percent who believe the institution president should oversee the CISO position.

Figure 35 depicts a comparison of four ideal reporting relationships according to CISOs and CIOs. Among both groups, the most frequently named ideal reporting structure was the CIO/CISO relationship, but the percentage of affirmative responses may reflect the opinion is not as widely supported among CISOs as it is with the CIOs. Less than half of the CISOs, 42 percent, listed that reporting structure compared to the vast majority of CIOs, 75 percent. While reporting to the president was the second most frequently choice for the CISOs, it was fourth for the CIOs. Clearly, there is a difference of opinion between the CIOs and CISOs about where in the organization structure the CISO belongs.
Four Most Frequently Selected Ideal CISO Reporting Titles, Figure 35

![Bar chart showing the percentage of CIOs and CISOs supporting various reporting structures to the CEO.]

Figure 35 The percentage supporting the various reporting structures reflect a difference of opinion about to whom the CISO should report. While both CIOs and CISOs named the CIO/CISO structure the most frequently, more CIOs supported that structure compared to CISOs.

The following Figure illustrates the reporting structure in terms of levels away from the CEO, zero representing a direct report. CHECS’ studies have consistently found that 97 percent or more of the CIOs reported within one level of the CEO. This CIO-CEO relationship has been a consistent result since 2003. While there is a great deal of information in the industry literature which suggests the CISO should report to the CEO, this arrangement has not become a reality for the majority of CISOs. Given the importance of this position and the number of information security threats directed against an institution, it is a concern that 65 percent of the CISOs report two or more levels away from the CEO.

CIO-CISO Comparison for Reporting Levels from CEO, Figure 36

![Bar chart showing the percentage of CIOs and CISOs reporting at different levels from the CEO.]

Figure 36 While a majority of CIOs report directly to or one layer away from the CEO, the majority of CISOs report two or more layers from the CEO.
IMT Membership

The institution management team (IMT) is the group of executives who lead the institution. This group may be called the cabinet, executive staff, or other term. Belonging to this group is often considered an indicator that the institution acknowledges the executive’s position is critical to the organization. Membership on this group may give the executive the ability to have a significant influence on the organization and, overall, raise their portfolio of responsibilities’ profile. In this research, 23 percent of the CISOs were members of the IMT (Figure 37). While some believe the CISO should be (or already is) a part of the IMT, in higher education this membership status is infrequent.

CISO IMT Membership, Figure 37

On the other hand, CIO membership on the IMT percentages have remained in the mid-fifty percent range since the early 2000s and 2015 was not an exception. In 2015, 57 percent of the CIOs were IMT members. Figure 38 depicts the comparison of CIOs’ and CISOs’ IMT membership and non-membership for 2015.
Almost three-fourths of 2015 CISOs were not members of the institution's management team. It is a sharp contrast with CIOs where more than half of them are members.

Considering the small number of CISOs who reported to the CEO and who served on the IMT, it can be inferred that they may not have a great deal of formal interaction with either the President or IMT. As Figure 39 depicts, only seven percent of the CISOs had weekly interaction with the President. Another 9 percent reported monthly interaction with the institution president and the majority, 54 percent, reported formal interaction occurred once a year or less.

The majority of 2015 CISOs formally interacted with the CEO once a year or less.
It is reasonable to surmise that an individual not serving on the IMT would have less interaction with that leadership group. Indeed, that was the case with the 2015 CISOs. Only seven percent of CISOs interacted daily with the IMT and another 15 percent indicated weekly interactions. The single largest percentage, 35 percent, interacted with the IMT monthly (Figure 40).

**CISOs’ IMT Formal Interaction, Figure 40**

![Chart showing CISOs' IMT formal interaction frequencies](chart)

*Figure 40 The majority of CISOs interacted with the institution's management team monthly, while less than a quarter of them had daily or weekly interaction.*

CIO/CISO interaction, however, occurred much more frequently. Thirty-five percent of the CISOs interacted with CIOs weekly, while another 50 percent interacted with the CIO on a daily basis (Figure 41).

**CIO Formal Interaction, Figure 41**

![Chart showing CISOs' CIO formal interaction frequencies](chart)

*Figure 41 CISOs interacted with CIOs more frequently than they did with CEOs or the IMT. Eighty-five percent of CISOs interacted with CIOs on a daily or weekly basis.*
CISO Preparation Activities

For anyone seeking to become a CISO in the future, knowing the best ways to prepare for the role may be critical. The CISOs selected activities they believed would be beneficial for someone who wanted to become a CISO. As in the 2014 results, the most frequently selected response (at 91 percent) was Professional development. Another 85 percent chose Mentoring and On-the-job training (Figure 42). In CHECS’ CIO research, the two most frequently selected methods to prepare for the CIO role were Mentoring and On-the-job training.

CISO Preparation Activities, Figure 42

![Bar chart showing the percentage of CISOs who selected different preparation activities: Professional Development 91%, Mentored by a CISO 85%, On-the-job training 85%, Certifications 73%, Other 14%, Actively pursuing next degree 14%.]

*Figure 42 In 2015, CISOs reported that Professional Development, Mentoring and On-the-job Training were the leading ways to prepare for the role.*

CIOs also provided their insight regarding the best ways to prepare for the CISO position. The CIO response mirrored CISO responses, naming the same top four activities (Figure 43).
Security Model

A security model is important to the CISO’s responsibilities, and the CISOs reported which security models they used. The two most widely used were NIST and SANS, with 59 and 57 percent, respectively (Figure 44).

Security Model Used, Figure 44

Figure 44 The majority of CISOs used SANS and/or NIST security models.
Knowing what security models CISOs used offers one point of view but just as important is knowing how valuable the CISOs considered their models to be. CISOs rated their security models from Least valuable to Very valuable. More than 60 percent of the CISOs found their security model to be Valuable while only 1 percent found their system to be Least valuable (Figure 45).

**Value of Security Model Used Figure 45**

![Bar chart showing the percentage of CISOs rating their security models from Least valuable to Very valuable.](attachment:chart.png)

**Security Program Maturity**

Many factors can have an impact on the maturity of the security program administered by the CISO. In CHECS’ research, only 13 percent of the CISOs considered their security program to be Mature or a Leader (Figure 46). Another 29 percent indicated their security program was Ad hoc or Under Development.

**Security Program Maturity – CISO, Figure 46**
More than half of 2015 CISOs believe their security systems were Improving while only 5 percent considered their systems to be a Leader.

The CIOs also provided their point of view about the maturity of their security program and their responses were similar to the CISOs’. Only 10 percent of the CIOs considered their security program Mature and none of them considered their program a Leader (Figure 47). Forty-four percent of the CIOs indicated their program was Ad hoc or Under Development.

Security Program Maturity – CIO, Figure 47

In this research, there were a group of CIOs who wore two hats; they were not only the CIO but also their institution’s CISO. Among that group, only six percent of CIOs considered their program to be Mature; while 61 percent of them viewed their program as Ad hoc or Under Development.
On the surface, these CIOs appear to be doing two very demanding and complex full-time jobs. Attempting to perform both of these functions may be too much for one person and, as a result, the program maturity may suffer.

**CIO also serving as the CISO: Security Program Maturity, Figure 48**

![Figure 48](image)

*Figure 48 For CIOs serving double duty as CISOs, their security program maturity may reflect the burden of one person trying to manage two complicated functions; 43 percent stated their program was Under development.*

**Security Program Resources**

The amount of resources devoted to an area can influence effectiveness. Moreover, the abundance or scarcity of resources may reflect the value the institution places on the area. The CISOs and CIOs provided data regarding the security program budget. Thirty-eight percent of the CISOs indicated there was not a dedicated security budget. Among CIOs, 57 percent indicated there was not a dedicated security budget. This lack of resources may be one of the reasons why a significant percent of the programs are still developing. The following three Figures depict program budget according to the CISO (Figure 49), the CIO (Figure 50) and a comparison (Figure 51).

**CISO: Security Program Budget, Figure 49**

![Figure 49](image)

*Figure 49 Thirty-eight percent of CISOs reported they did not have a security program budget.*
CIO: Security Program Budget, Figure 50

Figure 50 More than half of CIOs stated they did not have a designated security program budget.

CISO/CIO: Security Program Budget Comparison, Figure 51

Figure 51 A large percentage of CIOs and CISOs do not have a designated budget for their security programs. However, when a budget does exist, CISOs appear to have more resources devoted to their security program than CIOs do.

For the CIO who was also serving as the CISO, this study found that an even greater percent of them—75 percent—did not have a dedicated security budget (Figure 52).
CIO serving as the CISO: Security Program Budget, Figure 52

Figure 52 Seventy-five percent of CIOs acting as CISOs reported they did not have a designated security program budget, and of the 24 percent who did have a budget, 10 percent had a budget of less than $100,000.

In addition to a designated budget, this study also gathered information about a dedicated security staff. Fifty-one percent of the CIOs had employees dedicated to their security programs. Of those CIOs, 36 percent indicated they had only one person assigned to the security program (Figure 53).

CIO: Dedicated Security Program Employee, Figure 53

Figure 53 The majority of CIOs, 36 percent, staffed their security program with only one person; 35 percent had four or more dedicated staffing to their programs.

In sharp contrast, 81 percent of the CIOs who also held the CISO role did not have any dedicated staffing for their security program (Figure 54).
CIO serving as CISO: Dedicated Security Program Employee, Figure 54

Figure 54 For CIOs who also held the CISO position, only a small percentage had dedicated staffing for their security programs, while the majority did not.

Disruptions and Breaches

One of the key technology department responsibilities is providing and maintaining the availability of critical IT services. The CISOs and CIOs indicated whether or not their organizations’ were affected by service disruptions during the past three years. The results are depicted below in Figure 55. Twenty-four percent of the CISOs indicated they had been the victim of a disruption. Sixteen percent of CIOs indicated they, too, had experienced a disruption. Seven percent and five percent of CISOs and CIOs, respectively, declined to answer.

CISO/CIO: Disruption in Critical IT Services in Past Three Years, Figure 55

Figure 55 CISOs and CIOs responded to whether or not their organization had experienced a disruption in technology services within the last three years.

Another major concern for institutions is related to data breaches. Both CISOs and CIOs indicated if they had experienced a data breach in the past three years. There were 47 percent of the CISOs
who indicated they had experienced a data breach or declined to answer (Figure 56) and 31 percent of CIOs either experienced a data breach or declined to answer (Figure 57).

**CISO: Data Breach in Past Three Years, Figure 56**

![Figure 56](image)

*Figure 56 More than half of CISOs did not experience a data breach in the last three years, while 32 percent did.*

**CIO: Data Breach in Past Three Years Figure 57**

![Figure 57](image)

*Figure 57 CIOs fared slightly better than CISOs with 69 percent of CIOs indicating they did not experience a data breach in the last three years.*

While the results of this research cannot prove the lack of resources in a security program produces a less than satisfactory result, there is undoubtedly a connection. The institution where the CIO is also the CISO, where there is no dedicated budget and no dedicated security program employees are at a disadvantage in what is a very dangerous technology world with high stakes.
CISO Role Importance and Effectiveness

Role importance and effectiveness

The CISO holds a complicated position which is responsible for a wide variety of tasks. A number of sources were considered to develop a series of questions related to these tasks in order to help assess the CISOs’ roles and their effectiveness in those roles (Proctor, 2012; Scholtz, 2013a, 2013b, 2013c; van Zadelhoff et al., 2013; Whitten, 2008). In addition, the CISO members of the CHECS Advisory Board provided feedback.

The CISOs and CIOs responded to questions pertaining to CISO tasks and rated those responsibilities by “Importance” and job “Effectiveness.” The results were combined into six CISO roles. The CISO roles are depicted and defined in Table 7.

**CISO Roles, Table 7**

<table>
<thead>
<tr>
<th>CISO ROLE</th>
<th>RESPONSIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profession Advocate</td>
<td>Active in the professional and higher education community</td>
</tr>
<tr>
<td>Strategist</td>
<td>Develops programs and standards</td>
</tr>
<tr>
<td>Educator</td>
<td>Educates the institution on security policy and general security awareness</td>
</tr>
<tr>
<td>Traditional Security Operations</td>
<td>Framework implementation and incident response</td>
</tr>
<tr>
<td>Trusted Risk Advisor</td>
<td>Risk assessment and mitigation</td>
</tr>
</tbody>
</table>

Table 7 Six CISO roles were highlighted and defined in an effort to assess their role effectiveness.

To assess Role Effectiveness, CISOs and CIOs rated each of the roles on a scale of 1 to 5 for Importance: 1 indicated no importance and 5 indicated critically important. Likewise both groups rated themselves functioning in each role for Effectiveness: 1 represented expectations not met and 5 represented outstanding. These ratings are defined in Table 8.
CISO Role Importance and Effectiveness, Table 8

<table>
<thead>
<tr>
<th>IMPORTANCE</th>
<th>EFFECTIVENESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = No importance</td>
<td>1 = Expectations not met</td>
</tr>
<tr>
<td>2 = Least important</td>
<td>2 = Could be better</td>
</tr>
<tr>
<td>3 = Important</td>
<td>3 = Satisfactory</td>
</tr>
<tr>
<td>4 = Very important</td>
<td>4 = Excellent</td>
</tr>
<tr>
<td>5 = Critically</td>
<td>5 = Outstanding</td>
</tr>
</tbody>
</table>

Table 8 The ratings for role Importance and Effectiveness help to assess CISOs as a group and to measure the roles both by what the group considers to be vital and where improvement may be needed.

The aggregate CISO ratings of importance for the six roles are depicted in Table 9. All roles were rated as Important on the scale except for Strategist, which was rated as Very important. According to the CISOs, the two most vital roles were Strategist and Architect, which are proactive and higher order roles. The third most important role was Traditional Security Operations, which is a reactive and foundational role. As CHECS also found in its CIO role-importance research, the Educator and Profession Advocate roles were the Least important roles.

CISO Role Importance According to CISO, Table 9

<table>
<thead>
<tr>
<th>Role</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategist</td>
<td>4.02</td>
</tr>
<tr>
<td>Architect</td>
<td>3.78</td>
</tr>
<tr>
<td>Traditional Security Operations</td>
<td>3.58</td>
</tr>
<tr>
<td>Trusted Risk Advisor</td>
<td>3.54</td>
</tr>
<tr>
<td>Educator</td>
<td>3.52</td>
</tr>
<tr>
<td>Profession Advocate</td>
<td>3.34</td>
</tr>
</tbody>
</table>

Table 9 The Strategist and Architect roles are considered to be higher-order roles, while Traditional Security Operations is considered a foundation role.

Rating Effectiveness is a self-evaluation and the CISOs’ assessment of their Role Effectiveness is shown in Table 10. On the 1-to-5 scale described in Table 8, all of the self-evaluation ratings for each role were Satisfactory. CISOs considered themselves most effective in the foundational role of Traditional Security Operations, the third most important role, and least effective in the Educator role, their fifth most important role. According to the CISOs, the Strategist role, which was considered to be the most important, was fourth in effectiveness.

CISO: CISO Role Effectiveness, Table 10

<table>
<thead>
<tr>
<th>Role</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Security Operations</td>
<td>3.41</td>
</tr>
<tr>
<td>Architect</td>
<td>3.37</td>
</tr>
<tr>
<td>Profession Advocate</td>
<td>3.37</td>
</tr>
<tr>
<td>Strategist</td>
<td>3.21</td>
</tr>
</tbody>
</table>
Self-evaluation is only one component in the CISO role-effectiveness assessment. The CIOs’ evaluations of the CISO Role Importance is depicted in Table 11 and Role Effectiveness in Table 12. All of the roles were rated as Important on a scale of 1 to 5 (described in Table 8). The CIOs agreed with the CISOs on the three most important roles, although the second and third were in a different order. The most important role, Strategist, was followed by Traditional Security Operations and Architect. As with the CISOs, the CIOs ranked Educator and Profession Advocate as the least important roles. The Educator result is interesting considering that education is often cited as one of the best ways to prevent security incidents.

**CIO: CISO Role Importance, Table 11**

<table>
<thead>
<tr>
<th>Role</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategist</td>
<td>3.87</td>
</tr>
<tr>
<td>Traditional Security Operations</td>
<td>3.82</td>
</tr>
<tr>
<td>Architect</td>
<td>3.80</td>
</tr>
<tr>
<td>Trusted Risk Advisor</td>
<td>3.58</td>
</tr>
<tr>
<td>Educator</td>
<td>3.45</td>
</tr>
<tr>
<td>Profession Advocate</td>
<td>3.34</td>
</tr>
</tbody>
</table>

*Table 11 CIOs provided their opinions regarding CISO role effectiveness. Their responses were also collected in aggregate and a rating was calculated.*

Table 12 depicts the CIOs’ evaluation of effectiveness for the six roles. Four of the six roles were rated below a 3 on the 1-to-5 scale described in Table 8. The three most important roles according to the CIO, Strategist, Traditional Security Operations and Architect, were roles they rated the CISOs as most effective. However, Strategist was a 2.87, Could be better. Educator received the lowest Effectiveness rating, and this least effective rating was echoed by CISOs.

**CIO: CISO Role Effectiveness, Table 12**

<table>
<thead>
<tr>
<th>Role</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Security Operations</td>
<td>3.16</td>
</tr>
<tr>
<td>Architect</td>
<td>3.04</td>
</tr>
<tr>
<td>Strategist</td>
<td>2.87</td>
</tr>
<tr>
<td>Trusted Risk Advisor</td>
<td>2.85</td>
</tr>
<tr>
<td>Profession Advocate</td>
<td>2.77</td>
</tr>
<tr>
<td>Educator</td>
<td>2.75</td>
</tr>
</tbody>
</table>

*Table 12 CIOs provided their opinions about CISO role effectiveness. Their responses were analyzed in aggregate. CIOs and CISOs agreed on the top three principal CISOs roles, but not the role order.*

The following illustration depicts a side-by-side comparison between CIOs and CISOs role importance ranking as well as the role effectiveness.
Figure 58 The CISO and CIO aggregate responses are presented side by side for comparison.
Table 13 depicts a number of the CISO questions and the results for 2014 and 2015.

Higher Education Chief Information Security Officer for 2014-2015, Table 13

<table>
<thead>
<tr>
<th>Question</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age - percentage older than 51 years old</td>
<td>52%</td>
<td>43%</td>
</tr>
<tr>
<td>Female percentage</td>
<td>19%</td>
<td>15%</td>
</tr>
<tr>
<td>Minority percentage</td>
<td>5%</td>
<td>9%</td>
</tr>
<tr>
<td>Hispanic percentage</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Tenure in current position</td>
<td>3 years 10 months</td>
<td>5 years 3 months</td>
</tr>
<tr>
<td>Percentage with advanced degree</td>
<td>59%</td>
<td>58%</td>
</tr>
<tr>
<td>Percentage with technology major</td>
<td>35%</td>
<td>39%</td>
</tr>
<tr>
<td>Percentage retiring in 10 years</td>
<td>35%</td>
<td>35%</td>
</tr>
<tr>
<td>Reporting to CEO</td>
<td>4%</td>
<td>7%</td>
</tr>
<tr>
<td>Serving on IMT</td>
<td>18%</td>
<td>23%</td>
</tr>
<tr>
<td>Disruption in past three years – CISO</td>
<td>25%</td>
<td>31%</td>
</tr>
<tr>
<td>Breach in past three years – CISO</td>
<td>45%</td>
<td>47%</td>
</tr>
<tr>
<td>No dedicated budget – CISO</td>
<td>40%</td>
<td>38%</td>
</tr>
<tr>
<td>One FTE or less devoted to security – CIO</td>
<td>35%</td>
<td>36%</td>
</tr>
<tr>
<td>Security Program Maturity (Mature and Leader) – CISO</td>
<td>14%</td>
<td>13%</td>
</tr>
</tbody>
</table>
REFERENCES


Brenner, B. (2010, November 2). The New CISO: How the Role has Changed in 5 Years. CSO.


Slater, D. (2005, December 1). What is a Chief Security Officer. CSO.


About CHECS

CHECS was founded in 2009 by Dr. Wayne A. Brown to enable continued studies focusing on higher education CIOs’ attributes, education, experience and effectiveness. The research is unique from other CIO studies in that it is a two-part survey involving the CIO as well as other members of the institution management team. The annual study invites participation from the CIO (or lead technology person) at every two- and four-year higher education institution in the United States and internationally. Survey responses are analyzed in aggregate and statistical data is extracted and synthesized into an annual report. The CIO study has been conducted since 2003. In 2009, CHECS launched a second study focusing on those in the next organizational layer down from the CIO. This single-part survey is administered to higher education technology leaders to create the Higher Education Technology Leadership Study: The Chief Information Officers of the Future. CHECS is a nonprofit (501c3) organization dedicated to the education and development of the higher education chief information officer. It is an entirely volunteer organization and all studies are funded through report sales and sponsor donations.

In 2010, CHECS began funding a scholarship endowment to benefit higher education technology management doctoral students at Nova Southeastern University. CHECS funds a second scholarship endowment at University of Texas, Austin, to benefit undergraduate students seeking a higher education technology management degree. In 2014, CHECS began funding a third scholarship at Florida State University to benefit students in the Management Information Systems programs.

CHECS’ reports published in prior years may be ordered online. Credit cards are securely processed through PayPal. You do not need to have a PayPal account to use its payment processing system. Once an order is placed, a password-protected PDF will be e-mailed to the e-mail address you provide. Site licenses are also available. The license authorizes you to share the PDF with your institution. In addition, your institution will be recognized as a CHECS sponsor. For more information, visit CHECS online (www.CHECS.org).

CHECS gratefully acknowledges Dr. Detlev H. Smaltz. CHECS’ CIO survey was based on one created by Dr. Smaltz; the survey was modified and used with his permission.

Wayne A. Brown, Ph.D., is the Chief Executive Officer and Founder of CHECS. He has been a chief information officer since the mid-1990s and has worked in higher education at colleges in San Francisco, Kansas, and New York since 2000. Prior to his academic career, he was in the U.S. Air Force for more than 20 years, serving in the Medical Service Corps, Education and Training, and Security Forces. Dr. Brown began researching the higher education chief information officer roles and effectiveness as a doctoral dissertation and continued the surveys almost every year since 2003. Dr. Brown’s work has been widely published in higher education and technology publications, such as Chronicle for Higher Education, Information Week, CIO, Inside Higher Ed, Public CIO, EDUCAUSE Quarterly, League of Innovation in the Community College, EDUCAUSE Review, CIO, and Campus Technology, and he has presented research findings at technology conferences throughout the United States.