Crowe

Cybersecurity and Internal Audit

A Q&A With Lucas J. Morris, CISSP, and Christopher R. Wilkinson, CISSP

Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

The Internal Audit Foundation and Crowe, in collaboration with The Institute of Internal Auditors' (IIA's) Audit Executive Center, conducted a limited survey of IIA members in order to understand both the current and future role of internal audit in dealing with cybersecurity.

Expanding on their formal report of the survey findings, Christopher Wilkinson, a principal with the Crowe Technology Risk Consulting group, and Lucas Morris of Crowe discussed some additional questions about specific cybersecurity issues and trends that merit additional attention.

Q: Looking beyond responses to specific questions in the IAF/Crowe survey, did you find any broader trends or patterns particularly noteworthy?

Lucas Morris: One pattern that emerges when you dive deeper into the survey data is that the struggle to properly define internal audit's role in cybersecurity seems to be particularly challenging in midsize organizations.

For example, survey respondents rated the level of collaboration between internal audit and four other business units within their organizations – IT, information security (InfoSec), risk management, and compliance. Responses analyzed according to the size of the respondents' companies reveal that the relationship scores on average were noticeably lower in midsize organizations with between 1,000 and 5,000 employees.

Respondents rated relationships generally as more collaborative in smaller companies with fewer than 1,000 employees and in much larger companies with more than 5,000 employees. The middle tier of companies scored significantly lower.

Q: What accounts for such an unusual pattern?

Lucas Morris: I think the most plausible explanation is simply growing pains. In smaller organizations, members of the internal audit team are more likely to know peers in other departments. As companies grow, those personal relationships become less common.

On the other hand, in very large organizations, internal audit's role is more likely to be well-defined and structured, and, more likely, senior executive leadership represents internal audit in the C-suite. But in that middle tier of companies – those making the transition from small to large – relationship management is likely to present the greatest challenge.

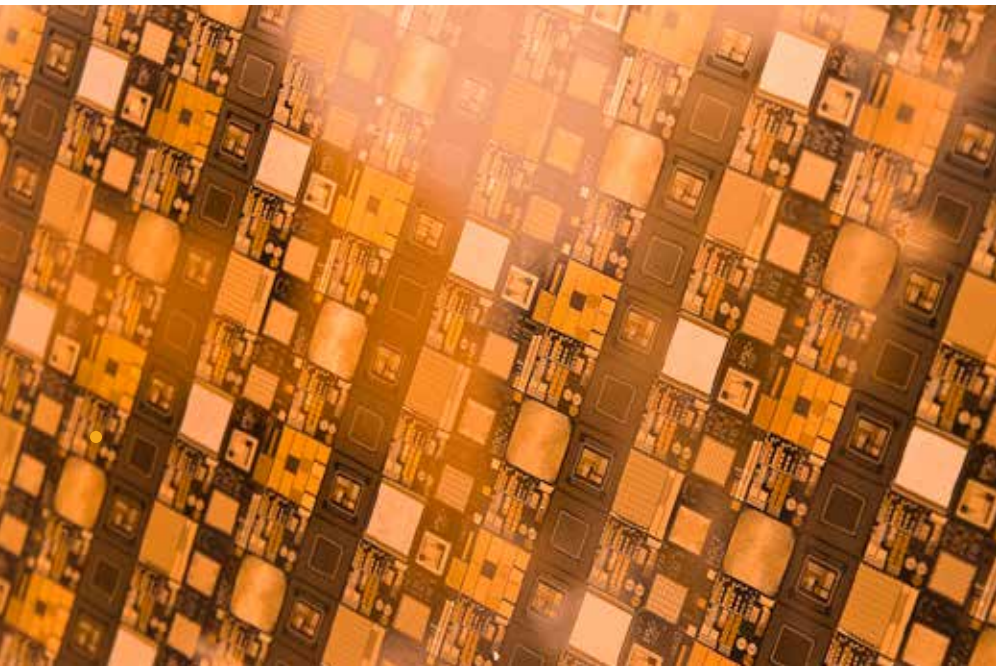
Q: Did any responses indicate areas of particular challenge for audit teams from smaller companies?

Christopher Wilkinson: Yes, several. One such area involved the level of attention given to cybersecurity trends by the board of directors and audit committee. When asked if they took steps to report cybersecurity risks and trends to these groups – that is, beyond standard audit reports – respondents from smaller companies were much less likely to say they did so.

It's important to point out that when the responses are broken down to this level, some sample sizes are relatively small, so we should try not to read too much significance into the numbers. Nevertheless, the broad pattern was unmistakable. Fewer than a third of the small companies' audit team members said they reported cybersecurity issues directly to their boards or audit committees.

Another area where smaller companies appear to have some catching up to do is in the use of penetration (pen) testing. Industry experience suggests pen testing providers are receiving many more requests for such services from small organizations than was typical a few years ago. But the survey still showed a noticeable drop-off in the use of pen testing services among smaller organizations.

Not surprisingly, virtually all of the larger organizations reported they use pen testing, but more than one-third of the respondents from smaller companies said their organizations did not perform such testing regularly. In fact, thinking beyond pen testing specifically, the broader category of specialized cyber assessments in general is an area in which internal audit departments in many smaller organizations could be taking a more active role, even though it might stretch their resources to do so.



Q: Speaking of resources, one major point in the final survey report was the importance of finding and retaining talent with needed technical skills. Does closer analysis of the responses offer any added insight into this issue?

Christopher Wilkinson: Yes, several responses were somewhat surprising. As might be expected, larger organizations overall were generally more likely to say they would be actively recruiting team members with certain specific technical skills in the next three years – that's no surprise. What was noteworthy, however, was the relatively large number of midsize and large companies that said they expect to hire people with specific expertise in IT governance and security information and event management (SIEM).

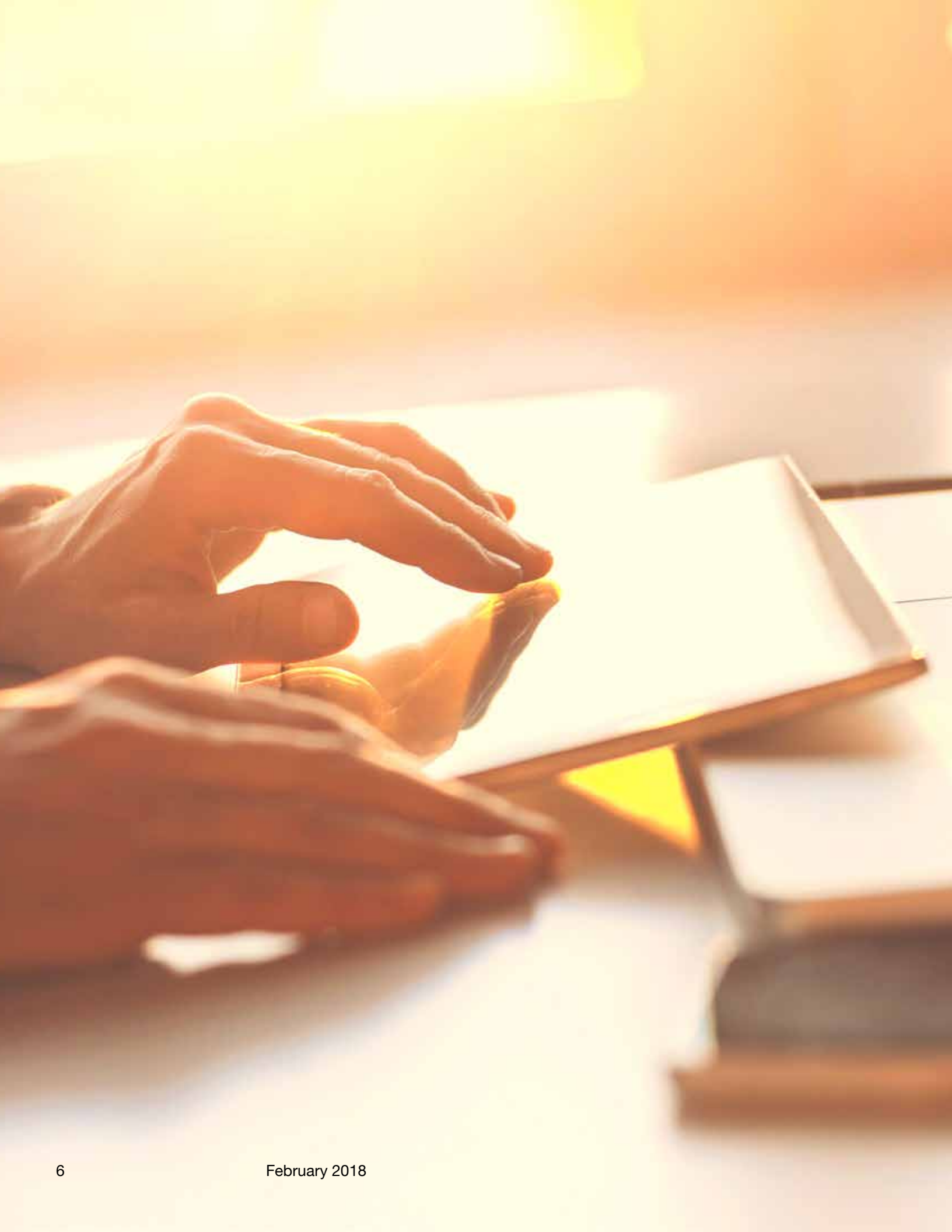
The need for audit team members with IT governance expertise is somewhat understandable because it's a fundamental element of IT and InfoSec operations. But SIEM expertise is a much more specialized area. It was a bit surprising, then, that respondents from large organizations indicated much higher levels of interest in hiring people with SIEM skills than they did in people with more widely used areas of knowledge such as Microsoft™ Windows™ Active Directory™ software, network configuration, or software development.

One possible explanation is simply that SIEM is a hot topic in IT circles these days. Auditors are likely to have heard their IT counterparts claim that their SIEM systems offer critical protection against any vulnerabilities their audits might have revealed. So some of internal audit's interest in SIEM might be simply a reflection of what they are encountering in the field.

A more likely explanation is that many larger companies believe they already have necessary skills in Active Directory software, networking, and software development, so they are now ready to begin augmenting their capabilities in more specialized areas. This explanation carries further credibility when we observe that smaller companies in the survey were more likely to predict continued hiring in the fundamentals than the larger respondents were.

One other somewhat surprising response was the number of internal audit departments in midsize and large companies that expressed an interest in hiring resources with pen testing expertise. Since pen testing is largely an outsourced activity, the need for dedicated internal audit resources with specific expertise in this area seems somewhat counterintuitive.

Again, since this response came primarily from midsize and large organizations, the most likely explanation is that audit executives in many of these companies are confident of their teams' basic skills, and they are looking to add specialized expertise.



Q: Beyond the specifics of hiring practices, reporting, and testing, the survey also asked audit executives several questions that were more strategic in nature. Any surprises in those areas?

Lucas Morris: Two survey questions in particular are worthy of attention. And here again, it appeared that midsize companies – that is, those with between 1,000 and 5,000 employees – are experiencing the greatest challenges in both areas.

Specifically, audit team members rated how actively their team consulted on major changes within the IT organization. Participants in midsize companies were much more likely to report they did not consult at all on such issues. In fact, midsize company participants were more than twice as likely to be excluded from IT change management decisions as their large company counterparts.

On another question, participants were asked if internal audit was a member – either voting or nonvoting – of project or IT governance committees. On this question, midsize companies were less likely to answer "yes." Once again, the challenges of establishing internal audit's important role in long-term change management and strategic issues were most acutely experienced in midsize companies.

Taken together, these questions indicate that navigating the transition from a small company to a large organization can be a particularly demanding task for audit executives.

Learn More

Lucas Morris
+1 214 777 5257
lucas.morris@crowe.com

Christopher Wilkinson
Principal
+1 214 777 5288
christopher.wilkinson@crowe.com

---

crowe.com

Text created in and current as of February 2018; Cover and artwork updated in May 2018.

RISK-18000-002C