Internal Audit's Role in Information Security: An Introduction
Transcript

Part 1: Internal Audit as Assurance Provider

Julia Allen: Welcome to CERT's podcast series: Security for Business Leaders. The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and executive outreach. Today I'm pleased to introduce Dan Swanson, President and CEO of Dan Swanson and Associates, and former Director of Professional Practices at the Institute of Internal Auditors. Today we'll be discussing the role of Internal Audit in helping build and sustain an effective information security program. So welcome Dan. Nice to have you with us today.

Dan Swanson: Thank you for inviting me to speak today.

Julia Allen: You're welcome. So let's start out, for our listeners who are not familiar with the role of Internal Audit, could you just briefly describe what it is and maybe some of the key responsibilities of audit executives or directors of IT audit?

Dan Swanson: Well internal audit varies across different industries and different size organizations, but fundamentally Internal Audit is there to do assessments of different operating practices of the organization and provide assurance to management and the Board that things are as people say they are. The other key priority is identification of improvement opportunities for the organization to implement.

Julia Allen: So what are some of the ways that the audit function maintains its objectivity in the organization and its independence, separation of duties, if you will? Because I imagine there's times when Audit can get very involved and times when they really need to step back. So how do they maintain that balance?

Dan Swanson: That's a very important issue for Internal Audit on a go-forward basis. First and foremost, the audit mandate, terms of reference, audit charter, if you may, is fundamental to establishing objectivity independence: the reporting to the Board, the reporting to the Audit Committee, sponsorship by the CEO, all contribute to the organizational function having objectivity independence.

Another key aspect is that Internal Audit should not do management activities, and that's a management function. So in Internal Audit efforts, over time, primarily it's an audit and assurance activity, although they do have some consulting engagements as well.

Julia Allen: So could you give me an example of maybe where some of the gray area might be, where it's clearly an Audit role or maybe clearly a role that Audit should stay away from? I suspect you've run into these from time to time.

Dan Swanson: Correct. Sometimes organizational units such as security, privacy, risk management, business continuity, need support from the audit function in enhancing the program and taking it to the next level. And based on a request from management and approval by the

Audit Committee on occasion internal auditors would participate in a consulting role for those functions. It's very important up front that management and the Board agree with that role for Internal Audit, and it goes back to the objectivity independence down the road. Typically Audit will be doing assessments and evaluations of the function and the programs and the efforts to identify gaps and recommendations for improvement. That's the core business of Internal Audit.

In security, the program is there to protect the organization from a privacy and security perspective, and the organization of that program and the assignment of responsibilities is a management activity and should be driven by management. Audit will typically consult, in an advisory capacity, in improving assignment of responsibilities.

Julia Allen: So that's a nice segue into maybe talking a little bit more in-depth about Internal Audit's role in security, information security, and privacy. And I suspect Audit deciding where to get involved and where not to get involved is probably also based on risk, wouldn't you say?

Dan Swanson: Fundamentally everything Audit does is risk-based. On an annual basis Internal Audit typically does a risk assessment of the organization to identify areas that they want to evaluate and report upon, in that assurance role; and then at a project level does a risk assessment at the front end of the project to ensure that internal audit evaluation is on the higher risk areas. Security is pervasive across the organization and therefore tends to be on the top-ten list of most audit functions, and as well could be incorporated into a variety of audits over the course of the year. If they're looking at the finance function, they could be looking at the security of finance information as a subset of that effort. So it really depends on how they organize the audit plan for the year.

Julia Allen: So it sounds like there are times when you're doing an audit on a mainstream business function, you used finance as an example, and you can certainly integrate some security considerations into that audit. Are there also times when you're looking at just security or privacy as a standalone audit objective?

Dan Swanson: Absolutely. I haven't read any surveys as far as the frequency of audit for security, but I believe in general that Internal Audit functions are looking at security, as a program audit or as a specific technology review, on a fairly regular basis. And the combination of those formal program reviews, formal technical audits, and then the audits in the other projects, the combination of those types of reviews supports that overall evaluation of the security efforts of the organization.

Part 2: Internal Audit as Collaborator

Julia Allen: Given your experience as an information security and IT auditor, what have you found or what have you seen to be some of the most effective approaches for putting an information security program in place, and Audit's role in helping do that?

Dan Swanson: I would say collaboration is the key. The security program across an organization of any size becomes a massive effort over a long period of time, and all to the value of reducing risk and improving protection of information. The audit function needs to determine their best bang for the buck and best approach to improving security, which is management's responsibility. Auditing the program would be an independent gap analysis, and that's typically done every two to three years.

And then on critical initiatives that every organization was working on, towards their strategic plan, including an assessment of the security implications as part of those reviews, is another key way of encouraging good security. And then working with security management directly on perhaps a

quarterly meeting of the two functions and what each are finding and what successes and challenges are being identified, is also very, very useful.

Julia Allen: Yes, I've often said in some of my conversations and presentations that information security professionals and managers should reach out and make Audit their new best friend, because sometimes I think Audit can deliver messages into the hierarchy of the organization that perhaps Security has a hard time getting anyone to pay attention to. Have you seen cases like that where Audit can kind of run things up the flagpole where Security really can't?

Dan Swanson: It does depend on the maturity of the program, the security program in the organization. If it's reporting into the organization at a lower level than perhaps it should be, sometimes an audit of security, one of the main issues is organizational status of the security function. Internal Audit has communication channels to the Board through the Audit Committee, so in that context can raise issues at the highest levels, which can be useful to both the audit function and the security function.

Julia Allen: So what types of security issues or concerns might an internal auditor, a director of IT audit, bring to the Board or senior executives? And when you do take an issue like that to the senior level what do you usually expect as a response?

Dan Swanson: Again it goes back to the individual organization and how Internal Audit's mandate has been defined, and how frequently we communicate to the Board. The first and foremost is the interaction between Internal Audit and management, in working through audit issues and audit findings and what management action plans are going to be.

So the first line of improvement is the communication between Audit and management. The second level is the periodic reporting to the Board on audit results, across the entire audit plan. And that assurance reporting should be communicating the essence of what the audits are finding and the important issues that the Board should consider in their activities. But there should be nothing new going to the Board that management's not aware of.

Now as far as specific issues, accountability for security is high on the list. The implementation of different technologies and practices from a process improvement and technical security is another big area. And then it goes back really to what the audits are finding and what management is reporting back as far as action plans.

Julia Allen: Okay, well that's really helpful because sometimes if you can kind of tackle the issue on multiple fronts and get different points of view to help deliver messages, that really I think can sometimes be a nice, sustaining feature to the security program.

So as we kind of get to our close, are there some steps or tips or ideas, maybe lessons learned, that you might recommend business leaders take to ensure that Internal Audit is, of course appropriate to their role and appropriate to the culture, is actively engaged in the organization's security program? If I'm a business unit manager what can I do to help Audit move that program along?

Dan Swanson: Well I'm a big proponent of management self-assessment for their program efforts. So having their internal view of the program and the gaps and the management actions required I believe is the first step of improving security. After that, or in preparation for that, asking Internal Audit to give their views on security is one level higher as far as an evaluation. If it's a formal audit, it eventually does get reported to the Board, at least significant findings do. And therefore you

really are asking for a report card that will become public at some point. So it's raising the bar in the sense of effectiveness of the program and the evaluation of the effectiveness of the program.

I think business leaders should encourage Internal Audit to provide opinions on information security. I think it's one of the top-ten priorities of most organizations. And Internal Audit should be providing opinions on key areas of the organization, key issues, key risks. And security is up there, with the best of them.

Julia Allen: So I know that you're a great resource for our community. Do you have some specific recommendations on where our listeners can learn more about this subject?

Dan Swanson: Well I do enjoy reading the material that CERT produces. The breadth and depth of the information on security is extremely extensive. The Institute of Internal Auditors and the ISACA, Information Security Audit and Control Association, are two key global audit communities that provide a wealth of information on the audit and assurance side. The Center for Internet Security was the - or is one of the key global organizations in relation to technical baseline security and technical assessments, and I highly recommend them as well.

Julia Allen: Well we'll make sure to include links to all of those in our show notes.

Well thank you very, very much Dan. This has been helpful, and I think will maybe serve as a nice introduction to our business leaders and security professionals to think a little bit more about how to make the best use of their internal audit resources. So I thank you so much for your time and expertise.

Dan Swanson: Thanks again for the invite.