Innovate Yourself

Using Innovation to Overcome Auditing Challenges

A couple of years ago, I made the statement during a presentation that the amount of information collected in auditing systems and controls is orders of magnitude greater than what we collected 10 years ago. This is just one challenge auditors must tackle as the pace of technology continues to move forward at a blistering rate. There are also new mechanisms and new standards. Technology itself, and the models and paradigms auditors have operated under for years, are undergoing a fundamental shift. At this point with cloud computing and the Internet of Things (IoT), auditors are awakening to a new reality, much like some 25 years ago to the explosion of the Internet.

How do practitioners cope? How do auditors continue to perform due diligence in the face of these increasing challenges? The answer, not surprisingly, is innovation. Everyone will have to become familiar with the new models, standards and technologies. In doing so, auditors can often find the answers to their own challenges.

More and More Data—Innovate With New Technology

Data are doubling every two years. One source cites that by 2025, data will double every 12 hours.[1] The two-year time frame is mind-boggling. Every 12 hours is unimaginable. However, it is well within expectation given how fast technology has gotten to every two years after centuries and millennia were the rate of data and information increase was slow and anything but steady.

Now data are collected on everything, even the performance of light bulbs. It is easy to develop means to collect, send and store data. However, once the data are stored, then what? There are various sayings in audit, and one of them is along the lines that if no one is looking at the logs, it is not an effective control. What if the situation is that no one is physically capable of looking at the data? For instance, many organizations are capable of capturing just about every packet that crosses their networks. Even with terabytes of storage, the captures can only be stored for hours or, at best, days. Contained within that data may be evidence of an adversary's actions. That data may also contain evidence of an issue with a control, such as a computer being able to access a resource on a restricted network when it should not be possible.

With that much data, it is unrealistic to expect a human or even a small group of humans to be able to process the network traces and glean the kinds of findings that are needed for audit. So how do auditors contend with this glut of data? Auditors should use the same technologies that business is using to achieve a competitive edge.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2nVSax1

K. Brian Kelley, CISA, CSPO, MCSE, Security+
Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camp, and user groups.

Enjoying this article?

- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

For instance, Not Only Structured Query Language (NoSQL) solutions such as those given the moniker "Big Data" provide significant computing power to find trends in data and detect anomalies. These provide actionable items for business. A *Forbes* article talks about artificial intelligence (AI) technology and auditors being in the same realm of capabilities. Basically, once the data are prepared, which is a typical step in a big data solution, then various mechanisms and algorithms are put to work to try to make sense of the data.[2]

From an audit perspective, practitioners have a good idea of for what they are looking. Therefore, if solutions are available and can be tuned to find this evidence, then auditors are capable of getting the information they need to either verify or question a control. Security software vendors have come to this same conclusion, and it is not unusual to find products built on NoSQL optimized for massive writes (the collection of data), which still provide an efficient means of accessing the information stored. Technologies such as Hadoop and ElasticSearch come immediately to mind.

> "MANY CONTENT DELIVERY APPLIANCES NOW HAVE MODULES WHERE THEY LEARN THE PROPER BEHAVIOR FOR AN APPLICATION AND THEY ARE ABLE TO FLAG AND BLOCK WHAT IS NOT NORMAL."

A Word About Continuous Monitoring

One approach the security community has taken is a concept called continuous monitoring.[3] Continuous monitoring works by knowing what is normal. When something that is not normal appears, it stands out. IT teams have used this idea for years to speed up troubleshooting. For instance, network engineers get used to what good connections look like at the packet level. When there is a problem connection, they spot it easily.

Likewise, senior web developers get very familiar with the request and response traffic between client and web server, and when they see a break in what is expected, they notice it almost immediately.

Obviously, with the amount of data generated, people alone cannot be relied upon. There is still too much data, regardless of how eagle-eyed a particular analyst, security engineer or auditor may be. Software is needed to do the spotting. This is called machine learning (ML) or AI. It is used everywhere now. For instance, many content delivery appliances now have modules where they learn the proper behavior for an application and they are able to flag and block what is not normal. AI is being used operationally for protection. It stands to reason that the same techniques can be used for verifying controls.

New Standards, New Protocols—Innovate Yourself

When auditors first started implementing web services, the protocol of choice was Simple Object Access Protocol (SOAP). Now many web services and application programming interfaces (APIs) use Representational State Transfer (REST). Part of the reason for the change is SOAP has a lot of rules. Among those rules is that data can be transferred only in XML format. XML format was once seen as the future of transferring data because it allowed users to describe the data and to enforce structure standards using a Document Type Definition (DTD). Any book from the late 1990s and early 2000s on e-commerce heralded the wonder of XML. Nowadays? Not so much.

One of the reasons REST has gained popularity is that it is not restricted to XML. HTML and JavaScript Object Notation (JSON) data formats are also acceptable. More and more, practitioners see JSON being used. For instance, if a user wants to define a custom security role in Microsoft Azure, he or she puts together a JSON file that lists what that role can and cannot do. Why JSON over XML? Quite simply, JSON follows an Agile axiom where just enough documentation is provided. A JSON file is simple. It does not have extraneous overhead. And it is human-readable, too, like XML. Therefore, the format is being used more and more. If a practitioner has learned how to read XML but not JSON, he or she is behind.

It is also important to talk authentication standards and protocols. In an era of open standards, Security Assertion Markup Language (SAML) got practitioners started. However, SAML underwent some major changes between versions 1.1 and 2.0. And now there is oAuth, oAuth2, OpenID and OpenIDConnect. Each of these protocols have different use cases, different formats, different terms, different strengths and different weaknesses. They are different. And IS auditors have to be familiar with them all.

I have just listed two areas where great change has taken place within the last few years. How does an auditor keep up? Auditors keep up by performing innovation on themselves. Within IT, the only constant is frequent and rapid change. Therefore, any practitioner associated with IT must be ready to frequently and rapidly change, too. This means setting aside time to learn and, basically, reinvent oneself with regard to what one knows.

The good news is that there are plenty of free and low-cost resources available to get up to speed on the latest standards. However, auditors still must take the time to take in those resources and process them. I know plenty of practitioners who make time as part of their day to play with the latest technologies; to understand new architectures, patterns and protocols; and to keep up with what the "cool kids" are working on and learning. This may not be part of their standard workday, but it is part of their day. They invest in themselves, even if it is outside of work hours.

When one thinks about it, this is what an innovation team is asked to do. It is asked to look at new technology and apply existing technology in new ways. The team requires time to learn and understand the technology and the use case, often experimenting with it as part of the learning process. Then they rapidly put it to use in a few test cases to see if it is viable and what can be learned from it. Practitioners can take those same principles and apply them to themselves.

New Technologies, New Rules

With the advent of new technologies, paradigm shifts are bound to happen. One shift for me was at a major security conference when the speaker talked about the network firewall as being insufficient.[4] He talked about protecting each asset, authenticating each asset and hardening each asset with its own firewall and protective rules. Just because someone is on the internal network does not mean they are trusted. He spoke about the fact that the concept of privileged networks that existed then (and still do now) would need to go away.

> "AUDITORS SHOULD EXPECT IT INNOVATION TO DEVELOP NEW TECHNOLOGIES WHICH CAUSE THEM TO ADOPT NEW RULES OF OPERATING."

He was talking about what is today called zero-trust security.[5] Cloud environments such as Microsoft Azure start with this model. With more interoperability, especially across untrusted networks such as the Internet, zero-trust security makes sense. With the ability of adversaries to compromise users using simple techniques such as phishing, zero-trust security makes sense. With the capability to automate configurations and push out updates and to implement Software-Defined Networking,[6] zero-trust security makes sense. However, zero-trust security is a massive paradigm shift from the "M&M" model of network security where the network firewall and Internet router represented the hard but then crunchy shell and the internal network and all of the resources deployed onto it the soft, chocolatey center.

Auditors should expect IT innovation to develop new technologies which cause them to adopt new rules of operating. This means a lot of new: new understandings, new controls, new evidence, new risk. Sometimes, learning conceptually about a technology is not enough. Learning and understanding the new model for which a new technology is applied is also necessary. This is a level beyond basic comprehension of facts. This also takes time and energy. Auditors should expect this to be part of their effort to innovate themselves. Sometimes, this means going back to a tabula rasa and asking the what, how and why questions for a particular technology. What is the technology designed to do? How does it work? Why does it work (or not work)? What problem is it trying to solve? Why do older technologies fail to solve the problem?

Innovation and the "New" Auditor

A one-line summary of this column is: Innovate yourself. As IS auditors, the technology world around us is going to continue to change at a breakneck pace. Data are increasing just as quickly, yet the audit role and responsibilities do not change. The nature of what auditors do stays the same. That means auditors need to continually learn the new technologies, models and paradigms. Auditors have to see how new tools and techniques help them keep up with the glut of data and the shift in how they operate. This is only done by continually innovating on auditors' own skills, by focusing on learning, by not letting perspectives and skills get stagnant, by asking the questions that need to be asked to go from just knowledge to understanding. Auditors are in an information age where knowledge workers rule. To be able to audit the knowledge workers, auditors have to be knowledge workers, too.

Endnotes

1 Libert, B.; M. Beck; "Leaders Need AI to Keep Pace With the Data Explosion," *Forbes*, 26 March 2019, *https://www.forbes.com/sites/barrylibert/2019/03/26/leaders-need-ai-to-keep-pace-with-data/*

2 *Ibid*.

3 CIO.gov, Continuous Monitoring, *https://www.cio.gov/agenda/cybersecurity/continuous-monitoring/*

4 Black Hat USA 2006, *https://www.blackhat.com/html/bh-usa-06/bh-usa-06-speakers.html*

5 Pratt, M. K.; "What Is Zero Trust? A Model for More Effective Security," *CSO*, 16 January 2018, *https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html*

6 Cooney, M.; "What Is SDN and Where Software-Defined Networking Is Going," *Network World*, 16 April 2019, *https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html*