IAITAM

APMG International
Accrediting Professionals

We had an opportunity to speak with Greg Witte, cybersecurity expert and one of the authors of the NIST Framework for Improving Critical Infrastructure Cybersecurity, about the importance of a robust IT asset management program as part of a cybersecurity initiative.

Q: Please tell us a bit about your current cybersecurity work?

A: I am a Security Engineer for G2 Inc., a Maryland-based team that seeks to help make a lasting positive impact by deliberately seeking and solving tough security challenges. I work with public and private sector organizations around the country, helping them improve their risk management processes. One of my key customers is the U.S. National Institute of Standards and Technology (NIST). G2 is the prime contractor for several divisions of the IT Laboratory. In that role, we collaborate with members of the security community, gathering information from around the world about what's working well, where security could improve, and what additional guidance is needed. Then we use that as the basis for research, tools, processes, and guidance.

Q: You were an author of the NIST Framework for Improving Critical Infrastructure Cybersecurity. What was the impetus for that document?

A: Back in 2013, as more advanced and more frequent cybersecurity attacks threatened us all, many in the U.S. recognized the need for a change of approach. The challenge didn't seem to be the need for more standards – we have had many of those, and attacks had increased despite many existing guidelines. Simply mandating rote compliance with controls wasn't the answer. So, the President issued an Executive Order and directed NIST to develop a Framework within one year. NIST received hundreds of responses to several Requests for Information, and thousands of attendees came to a whirlwind series of workshops around the U.S. Based upon lots of great comments and ideas, all drawing on proven standards and practices, NIST released the Cybersecurity Framework (NIST CSF) in 2014. More information is available from: https://www.nist.gov/cyberframework.

Q: While the framework was developed by a US federal government agency, NIST, can it be applied to the private sector?

A: Definitely! The original Executive Order that directed the creation of the NIST CSF recognized the need for better use of good practices and better information sharing among private sector organizations. NIST was directed to convene the workshops and publish the results, but the framework was built, and is being maintained, largely by the private sector for the private sector.

IAITAM

APMG International
Accrediting Professionals

Q&A

Questions for Greg Witte

Cybersecurity and ITAM

Q: The Framework Core highlights IT asset management as a critical area for control. How does cybersecurity benefit from IT asset management?

A: IT Asset Management (ITAM) is a critical part of cybersecurity. One might consider cybersecurity to be the process of protecting those IT Assets; (the data, IT-related personnel, devices, systems, and facilities that enable the organization to achieve business purposes) by preventing, detecting, and responding to attacks. When IT Assets are managed and monitored properly throughout the ITAM lifecycle, organizations are able to understand what should be protected and how. It is critically important that organizations identify and manage these assets consistent with the assets' relative importance to business objectives and the organization's risk strategy.

It's interesting to note that the benefits can work both ways. Often, the discovery and assessment capabilities of today's automated security products can help update ITAM inventory and monitoring. We often find that the most accurate inventory is one that draws upon multiple sources of information.

I think an interesting example is a recent comment from the U.S. Department of Homeland Security. In implementing their Continuous Diagnostics and Mitigation (CDM) program, the very first step they took was to require government agencies to better discover and manage hardware and software assets. Now that discovery tools have been deployed, the agencies have found huge numbers of uncatalogued and unmanaged computer devices connected to federal networks. DHS reported that some departments and agencies had "several hundred percent" more devices on their networks than they expected and the average across government was about 44 percent more. [1]

Q: In your work as a cybersecurity consultant, do you address the need to have a solid IT asset management process in place?

A: Yes. Since asset management is a critical part of cybersecurity, and because it's included as part of nearly every information security framework, we end up quickly discussing the need for solid IT asset management processes. The folks at the International Association of Information Technology Asset Managers (IAITAM) have taught me a lot about the ITAM lifecycle. We sometimes find that organizations are missing an opportunity to cover one or more elements of that lifecycle, including:

- Implementing policy and procedures for how IT assets should be requested and procured;
- Establishing rules about how and where to acquire assets to be used for critical/sensitive purposes;
- Defining IT assets themselves within the organization, including the possibility of including personnel, data, facilities, and infrastructure;
- Prioritizing those assets, such as through a Business Impact Assessment (BIA) and/or Privacy Impact Assessment (PIA);
- Defining the proper management of those IT assets, including access control, acceptable use, information protection, maintenance, monitoring, and incident response;
- Maintaining records regarding ownership and stewardship of the assets;
- Planning for the refresh and/or retirement of IT assets; and
- Ensuring the secure and responsible disposal of IT assets in accordance with their priority and with the sensitivity of any data contained within the IT system.

1 Department of Homeland Security official Kevin Cox at the McAfee Security Through Innovation Summit, hosted by CyberScoop.

IAITAM

APMG International
Accrediting Professionals

Q: How robust, on average, are the IT asset management practices in the companies you work with?

A: We usually find some good practices in place, but there's often many elements missing – possibly because there are varying definitions of ITAM. Many of the organizations have what I would consider to be a "property management" approach to ITAM. They focus on physical pieces of equipment that they can put a barcode label on and they move around once or twice a year with a laser scanner to update the inventory. The good news is: organizations that decide to think beyond the barcode will find that holistic IT asset management provides many benefits, including financial rewards.

Q: Do you think of IT asset management as going beyond just knowing what hardware and software you have in the enterprise?

A: Definitely. As I described before, each organization needs a well-organized approach that addresses the whole ITAM lifecycle. Just a glance at the well-known IT Infrastructure Library (ITIL) and IT Service Management (ITSM) models will demonstrate the breadth and complexity of information technology.

Q: Is IT asset management represented in commonly used security controls?

A: I believe that every commonly-used control model includes ITAM, from international standards like ISO 27000, to internationally recognized models such as the NIST Risk Management Framework or the CIS Controls for Effective Cyber Defense. Even there, we often find that the notion of ITAM is limited, while other portions of the lifecycle, like acceptable use of an IT asset, are covered in a different family. We'll have to keep working on that part!

Q: Do you find that IT asset management is typically a separate function from IT security, including cybersecurity? If so, how do you bring these groups together and harmonize their activities?

A: I think that these are often treated separately, but the functions really do harmonize, as I described above. Organizations would benefit from considering ways to better integrate ITAM with cybersecurity, and I would expect them to find some improvements in the process. For example, IAITAM advocates managing Total Cost of Ownership (TCO) by looking for ways to reduce the operational cost of IT (e.g., gaining efficiencies through data center modernization, "application rationalization" by identifying licenses across your portfolio not in use). The cybersecurity teams will find that this work to reduce TCO also helps to reduce cybersecurity attack surface. Eliminating unnecessary software also reduces potential software vulnerabilities.

Removing archaic business systems may also eliminate the insecurities of an outdated operating system.

It is important to remember that IT is increasingly becoming part of nearly every aspect of the organization. Where it once might have been relegated to the Accounting office, now there is IT nearly everywhere - the doors, security cameras, air conditioners, etc.

If an organization is implementing or updating processes based on a common framework, that might be an opportunity to have a discussion with multiple levels of stakeholders and intentionally look for actionable ways to integrate ITAM with cybersecurity. COBIT teaches that a good balance among Benefits Realization, Risk Optimization, and Resource Optimization is the way to meet stakeholders' needs. That's a good way to balance ITAM and cybersecurity, too!

IAITAM

APMG International
Accrediting Professionals

Q&A

Questions for Greg Witte

Cybersecurity and ITAM

Q: What do you see as the cybersecurity risks for companies who don't employ best practice for IT asset management?

A: Because many elements of cybersecurity are tied into good IT asset management, it is clear that what companies don't know can hurt them. Issues like "shadow IT", lack of mobile device management, rogue wireless/wired networks, and poor hardware/software maintenance can all introduce security vulnerabilities. It is also important to remember that there is always an adversary scanning the Internet for such vulnerabilities, so if you're not actively managing all of the IT within the company, there's a good chance that there's someone else somewhere on the planet who is.

Q: What advice would you give the C suite about implementing IT asset management best practice?

A: The first step, based on many of the frameworks with which I work, is a dialogue. Understanding both ITAM and cybersecurity as business needs with a technical aspect, rather than the other way around, is a great first step. After that, working with both ITAM and cybersecurity leaders, alongside the business leaders if those are separate, define the objectives and identify business-focused ways to measure progress. A business focus will help avoid the trap of just being compliant with one or more conformance requirements – one must comply with regulatory and contractual obligations, but that should be a side effect, not the primary goal. Organizations like G2 can help provide independent assessment and recommendations, and we can share what we've learned from other customers' successes. There are some great resources available, many at no charge, starting with IAITAM's IT Asset Knowledge site, http://itak.iaitam.org.

About IAITAM

The International Association of Information Technology Asset Managers, Inc. ("IAITAM") is the professional association for individuals and organizations involved in any aspect of IT, software and hardware asset management. Find out more at www.iaitam.org.

About APMG

APMG International is a global accreditation and certification body. APMG administers a range of professional assessment, development and certification schemes in key management disciplines including Business Relationship Management, PMD Pro – Project Management for NGOs and IACCM Contract and Commercial Management.

APMG works with strategic partners to provide access to best practice guidance, training and certification to help individuals and their organizations deliver positive results and change through improved efficiency and performance
www.apmg-international.com

IAITAM

Tel: +1.330.628.3012
Email: info@iaitam.org
Web: Web: iaitam.org

APMG International
Accrediting Professionals

Tel: +1 (0)781 275 8604
Email: info-us@apmg-us.com
Web: www.apmg-international.com