Q&A

EXECUTIVE VIEWPOINT
A Conversation with
SYED AZEEM

SYED AZEEM
Senior IT Project Manager,
General Services Administration

The senior project manager at GSA's Federal Systems Integration and Management Center talks about balancing cybersecurity and modernization

How can IT managers balance the need to secure legacy systems while modernizing their IT infrastructure?

One thing agencies need to do is rationalize their overall IT portfolios and consolidate the functionality around a select group of key systems or applications that can be based on a common mission area or on common user or stakeholder groups. This will not only reduce the overall attack surface that adversaries could potentially exploit, but it will also enable a renewed focus on ensuring that the right level of security investment and attention is being paid to the critical data that's housed in these systems.

A second strategy would be leveraging the greater economies of scale and potentially enhance security with cloud-based solutions. Certainly, cloud service providers are able to funnel the right kind of resources into security and spread those across numerous customers, and they're able to do that much better than the government can.

Last but not least, another strategy for small agencies might be to take advantage of security-as-a-service solutions wherever it makes sense.

At the end of the day, agencies should prioritize enterprise, rather than one-off, solutions as much as possible and try to cover the largest swath of users and use cases.

How can modernization enhance security?

IT modernization and cybersecurity really ought to go hand-in-hand. When modernization planning is done thoughtfully, the overall security posture for the organization improves dramatically.

When agencies are analyzing and comparing different products and technologies, what IT managers should keep in mind or pay close attention to are what built-in security features and solutions are available and also the compatibility of bolting on third-party solutions for current and future needs.

What security opportunities might agencies be overlooking in the rush to modernize?

When we're trying to achieve modernization and also better security, we need to adhere to fundamental cyber hygiene principles. If you look closely at the source of most of the recent federal data breaches – the successful attacks that have happened – almost always there's an element of good cyber hygiene missing.

For example, great strides have been made with privileged-user management in the recent past, and the federal government as a whole has been strengthening that in terms of stronger authentication, but strengthening authentication is only the first step. An opportunity could be, for example, where we apply advanced analytics, artificial intelligence-enabled behavior detection and also machine learning algorithms, so if there's any potentially anomalous activity that's going on outside the norm, that AI or those machine learning algorithms are able to detect it.

What tools and strategies could help agencies better manage the cybersecurity aspects of modernization?

While modernizing, agencies really need to take a closer look to see what pieces of the puzzle they can borrow without starting from scratch. For example, GSA offers a very robust shared identity management and authentication service for public-facing

The federal IT bench needs a **very strong project** and technical staff that is comfortable with the rapidly changing nature of technology.

online services. It's called Login.gov, and this was rolled out recently. Any agency can leverage it. It allows them to create a seamless and highly secure identity access management solution for primarily public-facing online services.

Other examples that are often overlooked are our bug bounties and ethical hacker services. Those can also be very valuable as a tool or strategy, and GSA's [IT Schedule 70] recently started offering a service for that, which is called Highly Adaptive Cybersecurity Services. That allows agencies to purchase specialized anti-hacker, ethical hacking services such as penetration testing, vulnerability assessments, cyber hunts, etc.

It's just a matter of being aware and making sure we're leveraging enterprise solutions that are already in place as much as possible.

What emerging technologies can help agencies improve their cybersecurity postures?

With the rise of tactical AI and machine learning solutions, agencies really need to start looking at these tools to enable better cybersecurity. For example, detecting insider threats is an extremely difficult problem to solve, so one of the tools they could employ is machine learning, which can detect behaviors and signatures associated with anomalous activity without the need for having to train an algorithm with structured data labels.

Another tool is behavioral analytics. It can help the security analyst be notified when there are behaviors that are out of the norm for privileged users. AI-enabled security tools can really allow the cybersecurity team to gain intuitive insights in real time, and that can be a great force multiplier.

Where do you think the cybersecurity focus will shift next?

A recent development that is encouraging is instead of being an afterthought, we're seeing a shift of security to the left of the life cycle. That means incorporating security throughout the life cycle as opposed to leaving it until the end, when the system has been developed, applications are good to go, and security almost becomes a hurdle. We're seeing a shift away from that and toward tackling security throughout the life cycle.

What common stumbling blocks are agencies experiencing as they modernize and secure their systems, and how can they address those challenges?

If I could point out one, it certainly is the workforce element. The federal IT bench needs a very strong project and technical staff that is comfortable with the rapidly changing nature of technology.

The technology landscape is pretty much evolving on a day-to-day basis. We need people who don't necessarily get comfortable with the status quo but are able to identify opportunities, provide capabilities and defend against threats posed by adversaries.

How can agencies find those talented professionals?

It all goes back to fostering a culture where the workforce of tomorrow is going to be motivated and empowered. That can't be overstated. Particularly members of the newer generation who are coming into the workforce need to expand how their work ties into the greater mission of the agency. But culture is something you foster over time.

Another issue is pay disparity. To address the skills gap, some agencies have taken innovative approaches. A select group of agencies has incentive pay for cybersecurity professionals, for example, and that's a great concept.

What emerging technologies are you keeping an eye on?

The lines are being blurred between physical control systems and software, and they're almost merging and bleeding into each other. Even at 1800 F Street — GSA's central office building — we are seeing the internet of things making its appearance. We have smart sensors located everywhere in the building. I'm really excited about the prospect of introducing connectivity and intelligence to the physical systems.

In terms of cybersecurity, it does raise a lot of serious concerns and things that have to be thought through, so it's always going to be a balancing act for agencies, industries and consumers to make sure that we're seeking the right balance between convenience and security and that we're not sacrificing one for the other. ■