PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

HOWARD WHYTE

CISO, NASA

HEADQUARTERS: WASHINGTON, DC

EMPLOYEES: APPROX. 61,000

Howard Whyte has performed the CISO role at NASA since October 2014 when he was appointed as "acting". Many others have held this position since the agency's first CISO took office a few decades ago. "Most NASA CISOs are in the position for 2-3 years. This is a highly visible and stressful job as we protect the security of the space mission. There is pressure to get it right all of the time, while our adversaries only need to get it right once," said Whyte.

One way Whyte attempts to diffuse the anxieties of the job is by engaging the entire NASA team in security efforts. "If you don't have support from the top all of the way down to program support it can be very stressful," said Whyte. "We have to make sure agency executives, and system admins who have control of the technologies, are clear on their role in protecting our mission. They each have to know how they can help to minimize our attack surface."

To ensure the agency employees effectively participate in security efforts, Whyte maintains a focus on education and awareness. "I have regular, direct communication with everyone in the agency. I get out and meet folks, and I run all-hands meetings to explain how each team member fits into the security strategy."

CHALLENGES TO THE ROLE

"Our biggest challenge is that we are a federated environment, that means we have multiple centers with their own authority and resources," said Whyte. In fact, while Whyte is the NASA CISO and reports to the agency CIO, each of the ten centers across the US have their own CISOs and CIOs. Whyte must work closely

with each Center's CIO and CISO, setting security strategies and standards for the agency. "We have to focus a lot on collaboration. We have to get out in the field and not be empirical. We need to work with those in charge of running NASA's missions to make sure security objectives are met across the board – whether on the ground or on the space craft."

A big challenge that Whyte is facing, together with his security professional peers, is moving beyond the tactical security approach of reducing threats to understanding the value of data and how to safeguard it. "NASA has endured a lot of attacks, from all kinds of hacktivists, nation-states and people just looking for notoriety. We have to be concerned with the full spectrum of breach and react based on the risks we face every day," said Whyte. While threats will always be there, Whyte believes that in the next five years he and the security community will become more focused on data protection, instead of threat detection and prevention. Whyte worries about the cloud eco-system, and he prioritizes understanding who has access to agency data and how they use it. "Data protection requires risk management. You need to know what you have and the value of that data, then conduct the needed assessments to ensure that cost effective measures are in place to protect it. Effective risk management demands all stakeholders (internal and external) work together to tackle risk from an agency-perspective and not just from a security standpoint. You should be aligned with the Agency strategy and mission objectives and work with the IT Security steering committee and business leaders to make sure you allocate security resources to reduce the risk to our assets."

WHEN A BREACH HAPPENS - Delivering the Bad News

Whyte's image as a Security Ambassador for NASA was of benefit recently when he acted as a liaison between NASA and the Office of Personnel Management (OPM), while they reacted to their own significant breach. Though the breach exposed personal data of NASA employees, it did not impact NASA systems. The NASA security team was not in control of the breached systems. "My role was to be an information conduit, taking updates and information from the OPM security team and delivering the information to NASA's stakeholders." In addition to making sure NASA's employees were aware of the extent of the breach, and the protections available to them, Whyte is tasked with ensuring the exposed data is not used to socially engineer an attack on his systems. "We really need to be diligent in making sure that countermeasures are in place to protect networks, systems and information," said Whyte.