How employees can **boost cybersecurity**

The right monitoring controls and a well-trained workforce can go a long way toward improving security

Jim Hansen
Vice President of Products, Application Management, SolarWinds

DESPITE THE CHANGES brought by the COVID-19 (or coronavirus) pandemic, agencies still have to deliver necessary services, including those to support national defense and health care. However, their budgets are stretched thinner than ever because they must find new ways to deliver those services.

As a result, the need for scalable cloud environments has become more urgent.

However, government cybersecurity challenges are evolving along with the network. Adversaries are constantly learning how to take advantage of new mechanisms to infiltrate IT infrastructures more effectively and avoid detection, and they're capitalizing on agency networks becoming more dispersed.

Recruiting security experts from the IT ranks

Security controls are even more important in a world of perimeterless IT environments and expanding cloud adoption. Agencies need to appropriately budget for cybersecurity and apply the basic hygiene of security patching and vulnerability assessment. Those steps can cover about 80% of basic threats, and the security team can focus its energy on more complex threats.

Having a strong team is the foundation of those efforts, but it's not easy to recruit private-sector cybersecurity professionals for government jobs. An alternative is to recruit from within. The government should consider creating programs to train IT team members to take on higher-level cybersecurity roles, which helps agencies build effective teams and helps employees progress on a career path. Whether they bring in new talent or train existing employees, agencies must offer competitive salaries and benefits to keep cybersecurity professionals satisfied and engaged.

A zero trust approach to the world

Protecting against insider threats, whether malicious or unintentional, comes down to proper monitoring of the infrastructure and assets employees are accessing. For example, SolarWinds® Access Rights Manager helps agencies know what their employees are doing while they're connected to an on-premises network or cloud environment and highlights when somebody does something out of the ordinary.

Sometimes users aren't actively trying to circumvent the agency's controls but unintentionally create a cybersecurity risk. Agencies should take advantage of the opportunity to teach them cybersecurity expectations and train them to be vigilant in a digital world where everybody wants to steal government information. This attitude forms the basis of a zero trust approach to IT and the world in general.

If they operate under the assumption that they cannot trust anyone or anything and apply security controls accordingly, agencies can save time, money and effort in discovering and containing threats whenever they appear. ■

Jim Hansen is vice president of products for application management at SolarWinds.