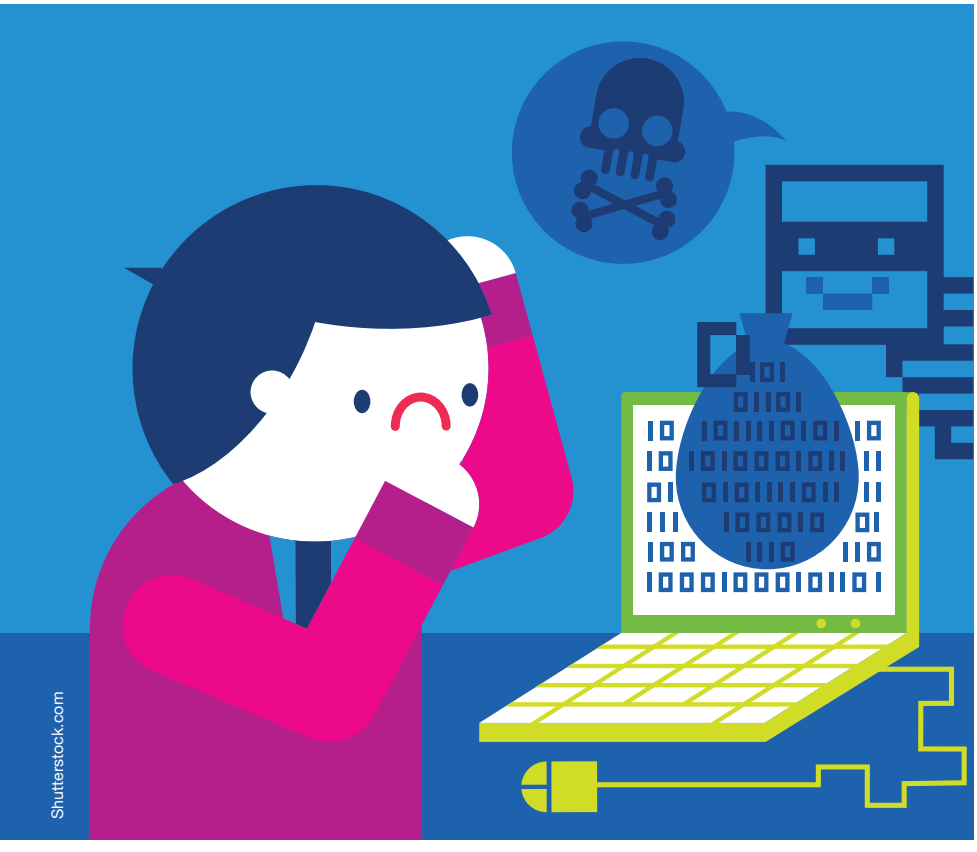
SPONSORED CONTENT

Take Cybersecurity to the Next Level

A risk-based approach leveraging automation is one of the best ways to give your cybersecurity posture a solid foundation.

A top challenge for every government agency today is the effective management of cybersecurity risks. Protecting government information and citizens' personal data has become more challenging as our networks and the amount of data on them has grown exponentially. Integrated, automated response to the growing wave of cyberattacks is the only way for network defenders to keep up. Best practices from the National Institute of Standards and Technology (NIST) offer a proven approach to cyber risk management. They guide you toward the right cyber investment decisions that help reduce risk to acceptable levels for your specific agency.

Government agencies rely on technology to complete their missions each day. However, this technology has also grown more complex and diverse over the years. There are now more endpoints, greater reliance on the cloud and enhanced mobility. These advances improve productivity and efficiency, but also make the job of network management a more complex endeavor. Instead of simply protecting a set of applications and data within a defined perimeter, government agencies today must also protect the sensitive information that leaves the traditional perimeter though cloud applications and mobile devices.



Shutterstock.com

At the same time, cyber-attackers have become more aggressive and sophisticated. They're constantly finding new ways to infiltrate networks and steal both intellectual property and private citizen information. The sheer volume of Distributed Denial of Service (DDoS) attacks, which can shut down a network, also are on the rise.

Agencies at all levels of government are dealing with these changes. A report from KPMG and (ISC)2 , for example, found 65 percent of federal cyber executives don't believe the federal government is equipped to detect ongoing cyberattacks.[1]

On the state and local level, a report from Deloitte and NASCIO[2] found more than half of state officials aren't confident their state's information assets

are protected from cyberthreats. This lack of confidence largely stems from the use of emerging technologies like cloud and Internet of Things (IoT).

Another reason government officials aren't as confident as they should be is because agency networks have grown and changed. They've added network security technologies at different points to address different threats. According to a recent CSO report, an average of 89 different vendors accessed the average organization's network every week.[3] And only one-third knew the exact number.

With that many disparate security solutions, it's difficult to find sufficiently knowledgeable personnel. It's also difficult to manage and easy for vulnerabilities to fall through the cracks. "You can't take a piecemeal approach to security today," says Peter Romness, Cybersecurity Solutions Lead for the Public Sector at Cisco Systems. "You have to look at everything holistically—as a risk-based decision, just like any other business decision."

"You can't take a piecemeal approach to security today, you have to look at everything holistically–as a risk-based decision, just like any other business decision."

To maintain optimal effectiveness, network security today must be simple, open and automated:

Simple: Easy to deploy, manage and scale. Easy to understand and act on the output of cybersecurity solutions so that threats can be detected and remediated quickly. Easy to insert into existing environment while minimizing network impact.

Open: Use open standards and APIs to ensure products interoperate. One example is Cisco's Platform Exchange Grid (pxGrid), a multivendor, cross-platform language that lets a set of APIs remain the same from product to product. If Cisco or any other company writes to those APIs, it will work with pxGrid, as well as all other solutions.

The Cybersecurity Workforce Problem

According to the 2016 Deloitte-NASCIO Cybersecurity Study, more than half of state and local agencies say there aren't enough cybersecurity professionals to satisfy their requirements. The study also found 56 percent of the cybersecurity professionals on staff had competency gaps. The same is largely true in federal government. These issues are the result of demand from other agencies and the private sector, and because our schools can't train them fast enough.

Again, NIST comes to the rescue with its NICE Cybersecurity Workforce Framework[4], a national initiative for cybersecurity education. This new approach not only defines the different cybersecurity roles agencies require, but explains the knowledge, skills and abilities required to fulfill each role.

The NICE Cybersecurity Workforce Framework is an excellent companion resource for the NIST Cybersecurity Framework, says Cisco's Steve Caimi. "The Cybersecurity Framework addresses the essential people, process and technology controls, but it does not discuss the roles or skills you need to accomplish all that's required," he says. "That's where the Workforce Framework comes in. It addresses the specific knowledge, skills, and abilities that an effective cyber workforce really requires."

Automated: Act immediately when the cyberattack strikes. Exploits often succeed in a matter of minutes, faster than even the most seasoned cyber professionals can see and react. Automated detection and response action balances the people, process, and technical controls in your agency to deal with today's highly sophisticated cyberattacks.

Reducing complexity, ensuring products work together and automating to the greatest possible extent is the best way to ensure better cybersecurity. "If the day-to-day activities are automated, then threats that need more attention are highlighted and network operators can make better decisions," says Romness.

This Doesn't Mean Starting Over

Making networks fully cybersecure doesn't mean throwing everything out and starting over, says Steve Caimi, a specialist in U.S. Public Sector Cybersecurity at Cisco Systems.

"NIST has been at the forefront of cybersecurity best practices, especially since FISMA was enacted and NIST developed Special Publication 800-53," he says. "More recently, the NIST Cybersecurity Framework[5] is an extremely effective way to assess the risks to your organization from a cyber perspective and guide you to where you should invest."

NIST's Cybersecurity Framework outlines the people, processes and technology controls that are essential for an effective cybersecurity program. It's organized around five core functions: Identify, Protect, Detect, Respond and Recover.

While it's true no organization can ever be 100 percent cybersecure, agencies can and should do their best to bring risk down to an acceptable level.

While every government agency at every level faces different threats and types of risks, the Framework helps organizations assess where they are, and identify the biggest risks to their particular organization. It's so effective the Commission on Enhancing National Cybersecurity recommends it become mandatory across the federal government. Gartner estimates that by 2020, more than 50 percent of organizations, both government and commercial, will have adopted the NIST Cybersecurity Framework. That's up from 30 percent in 2015.

Before making any changes, Caimi recommends agencies at all levels of government assess their agencies with a true understanding of the Cybersecurity Framework. The next step is using the processes it outlines to improve the cybersecurity program and determine where to focus.

Using existing best practices like the NIST Cybersecurity Framework to review what is already in place and analyze current risks and threats is a good first step to improving cybersecurity. While it's true no organization can ever be 100 percent cybersecure, agencies can and should do their best to bring risk down to an acceptable level.

And once cybersecurity is under control, it becomes an enabler for the true promise of IT. "If you can be confident that your data, IP and networks are secure, you can feel much more confident about providing new services to your citizens," says Romness.

For more information, please visit: cisco.com/go/security.

[1] www.isc2.org/fedcyberexecsurvey/default.aspx

[2] www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress

[3] www.csoonline.com/article/3055012/techology-business/only-a-third-of-companies-know-how-many-vendors-access-their-systems.html

[4] csrc.nist.gov/nice/framework

[5] www.nist.gov/cyberframework