SPONSORED CONTENT

INNOVATION FUELS CYBER ADVANCES

New technologies and strategies provide government agencies with new ways to defend their networks.

FOR GOVERNMENT AGENCIES looking to improve their cybersecurity, innovation is the order of the day.

It's not just that today's cyber threats are more sophisticated and numerous than ever before. It's also that the IT environment has grown more complex, as agencies have expanded their use of cloud, mobility, the Internet of Things and other solution areas.

This complexity, which creates a more extensive attack surface for bad actors, requires agencies to think in new ways about cybersecurity. Their existing tools might be sufficient for the intended purposes, but new tools, tactics and strategies are needed.

Fortunately, recent months have brought a surge in innovation, as agencies at all levels of government have explored new possibilities for strengthening their cyber posture. Here is a look at some of the hottest areas of activity.

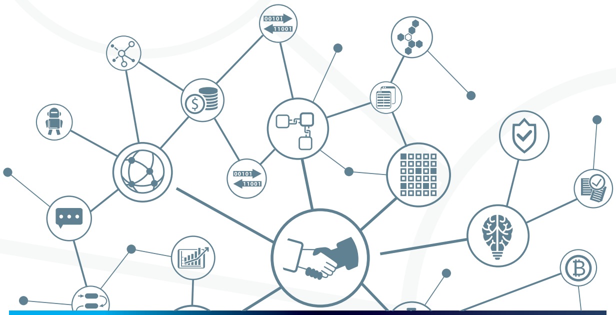
Data Sharing and Analysis: Cyber Warning Systems

The proposition seems simple: The more information that agencies have on cyber threats, the better prepared they will be to protect themselves. In practice, however, agencies often have struggled to implement the necessary policies, procedures and technologies needed to aggregate and analyze data from different sources. But that is beginning to change.

Los Angeles, for example, is launching an organization called CyberLabLA that eventually will facilitate the sharing of information among public and private sector organizations. Additionally, the city plans to build on that work by creating a Cyber Lab Innovation Incubator, which will include a simulated city network that can be used both to test new cyber defenses and to train cyber experts.

Michigan, on the other hand, is looking to take a longer view, trying to leverage its historical cyber threat data to become more effective at predicting emerging threats. The center will work with data generated by a wide variety of systems, such as firewalls, security appliances and intrusion detection systems, as well as data available through commercial services. The goal is to create models that, when applied to current cyber data, can point experts towards emerging threats.

Still, more work needs to be done on the policy front, experts say. A key concern is overcoming institutional barriers to information sharing between the public and private sectors and across different levels of government.



Blockchain: Foundation for Digital Government

To be fully realized, the vision for digital government is built on trust—trust in the integrity of digital transactions. That is, how can a citizen or organization be sure that data has not been tampered with in the course of a transaction?

One promising solution is blockchain technology. Blockchain is generally described as a distributed, trusted ledger of transactions. Each step of a transaction is validated by a participating node, with each validation linked to previous validations, forming a chain. If the transaction is intercepted by an unauthorized party, the chain is broken—and everyone knows it.

Because the ledger travels with the transaction, it does not require centralized management—which makes blockchain more easily scalable than alternative approaches, such as public key infrastructure.

The National Association of State CIOs has flagged

blockchain as a promising solution. "As blockchain continues to evolve, state governments can start taking advantage of the technology to improve their services and supply chains through pilot programs," according to a recent NASCIO report, "Blockchains: Moving Digital Government Forward in the States."

A growing number of government agencies are exploring the possibilities. The Illinois Department of Innovation and Technology is working with state and local agencies to develop use cases for the technology. In a similar vein, the D.C. Blockchain Center is bringing together government agencies and industry experts around the nation's capital to do similar work.

The U.S. Department of Homeland Security is also getting involved. The department's Science and Technology Directorate is funding startups that could help address gaps in current blockchain solutions.

Federal R&D: Botnets, Cryptography and More

Indeed, despite the booming industry for security solutions, the federal government continues to play an important role in seeding the market with new technology or funding the work of entrepreneurial vendors.

For example, the Defense Advanced Research Projects Agency (DARPA) is focusing its energies on so-called social engineering attacks, which are designed to trick people into clicking on a link that downloads malware.

Government agencies often require employees to take training that includes a session on social engineering, but the results are decidedly mixed. Humans continue to be seen as the weakest link of any cyber strategy.

DARPA proposes using bots to detect a social engineering campaign and to identify and gather information about its source. "To build secure cyber systems, it is necessary to protect not only the computers and networks that make up these systems, but the humans as well," the broad agency announcement states.

In some cases, the problem is not that cyber solutions don't exist—it's that they are difficult for many people to deploy. That is the case with some advanced cryptographic techniques.

With that in mind, the Intelligence Advanced Research Project Activity (a DARPA-like group for the intelligence community) hopes to create a cryptographic toolbox that systems architects and application developers can use even if they lack cryptographic expertise.

The program, called the Homomorphic Encryption Computing Techniques with Overhead Reduction, or HECTOR, likely will include cryptographic tools, programming languages and design and verification tools.

But in some cases, federal agencies take a more measured approach to driving the development of solutions. For example, the National Telecommunications and Information Administration (NTIA), which is part of the Commerce Department, is seeking industry partners interested in developing new strategies for dealing with automated distributed attacks from botnets and related technology.

For starters, NTIA wants to assess the effectiveness of current solutions—both in terms of what works and what gaps need to be filled. But the agency also wants to get feedback on what roles the government should play in filling those gaps. Its findings will be included in a report due by January 2018.

Back to Basics

While innovation is critical to the future of cybersecurity, the WannaCry ransomware incident in May was a reminder about the importance of basic cyber hygiene.

The designers of WannaCry exploited known vulnerabilities in commercial software. According to U.S. intelligence officials, few U.S. government agencies were infected, thanks to their disciplined approach to managing software. In contrast, organizations that failed to apply patches or upgrade their software paid the price—literally.