Security progress **one step at a time**

Modernization shines a light on alternatives to all-or-nothing approaches to encryption and cyber strategies

Rob Roy
Public-Sector Chief Technology Officer,
Micro Focus Government Solutions

THE GOVERNMENT SPENDS roughly 75 percent of its IT budget to operate and maintain systems that in some cases were created decades ago, instead of investing in innovative new technologies and capabilities that will move the government forward and protect existing assets.

Older systems lack modern cybersecurity standards, so they are ripe targets for adversaries. In fact, making new and old systems work together is an essential component of modernization. In some cases, agencies will choose to replace a legacy system with something new. However, for cost, complexity or security reasons, many agencies will choose to leave the data in place on the old system and write a front end to it to take advantage of the security, performance and reliability of cloud-based applications.

Rebuilding applications in that way allows agencies to maintain control over their data and represents a perfect use and cost-effective application of IT modernization. The push to modernize is a valuable opportunity to take a fresh look at systems and security.

A new encryption model

Securing data will often prevent seamless access for employees and partners unless the right technology is selected. Much of the available technology uses an all-or-nothing form of encryption. With those technologies, an entire record is encrypted, and certain users or roles within the organization have the ability to unlock all the information, which means that an attacker who obtains the appropriate credentials can also unlock everything.

There is an alternative. Format Preserving Encryption (FPE) with Micro Focus SecureData has been tested and used for over a decade by major enterprises and has the stamp of approval from the National Institute of Standards and Technology for government use.

For example, FPE can selectively encrypt data on credit card holders in a company's database. Users or administrators can view only enough data to help service the card holder's account, which also restricts the access of hackers who might obtain a user's credentials.

The format-preserving nature of FPE has distinct advantages. Other forms of encryption typically expand a credit card or Social Security number into a very large, random set of characters that no longer fits in the database, which leads to the myth that encryption requires a completely new architecture. With FPE, a credit card number is encrypted and put back into the database with 16 digits or a Social Security number with nine digits. No changes to the underlying database are required.

That means multiple systems can use the same database without having to rewrite the format, and organizations can open datasets to partners without having to scrub sensitive

deepOV/RedlineVector/Shutterstock/GCN Staff

The push to modernize is a **valuable opportunity to take a fresh look** at systems and security.

personal information because those partners can only view enough of the data to fulfill their missions.

Learning from the cyber sprint

After the massive Office of Personnel Management breach in 2015, then-CIO Tony Scott took advantage of the opportunity to make fast progress on improving agencies' security postures.

For the 60-day cybersecurity sprint, a little bit of money was reapportioned to help every agency in the federal government radically accelerate a few primary improvements. One was patching all the weaknesses they knew about, and another was adopting multifactor authentication for privileged users. Agencies overwhelmingly succeeded in both areas.

IT leaders do not need to tackle cybersecurity all at once. In fact, the push for modernization gives them the opportunity to make incremental progress a regular occurrence. As they are updating their systems, agencies should also be prioritizing and reducing cybersecurity risks one step at a time. ■

Rob Roy *is public-sector chief technology officer at Micro Focus Government Solutions.*