Sabre Schnitzer, Manager, Compliance, Veritas Public Sector

Q&A
Building a Better Data Management Strategy
Step Three: Secure

State and local governments store a significant amount of data that is highly valuable to cybercriminals. The potential for a breach that would impact citizens, impair government operations and damage public trust has made secure data management a top IT priority.

When developing a game plan for data management, three steps are critical for success: design, manage and secure. In this Q&A, we take a closer look at step three: secure. Manager of Compliance Solutions for Veritas Public Sector Sabre Schnitzer discusses how governments can strengthen their overall security posture and data protection efforts.

Q: What do governments often overlook in their data security measures?

The first issue comes with moving data to the cloud. Agencies are increasing their use of public cloud services to run selected application workloads and maintain scalable data archives. Although a cloud provider may meet security requirements, agencies still need to identify which data is appropriate for cloud storage and establish proper governance policies and procedures.

The second concern comes with online service portals for citizens. IT needs technology that protects citizen information while also preventing someone from using the portal as an entryway for unauthorized access to other sensitive data or applications.

Finally, because IT staff are often stretched thin, application patching isn't always done in a timely manner. When patch processes aren't automated, data and applications are vulnerable to a breach or ransomware attack.

Q: What can IT do to improve data security?

An initial step is to implement a continuous security monitoring capability across the IT infrastructure. This monitoring program can identify easy-to-fix issues such as needed application patches or users who haven't updated passwords.

The next step is to consider adopting cybersecurity frameworks published by the National Institute of Standards and Technology (NIST) or the Defense Information Systems Agency (DISA). These frameworks offer a comprehensive view into security best practices across IT products and applications, as well as the network and cloud. Their detailed guidelines also help an agency assess its current security measures and identify needed changes in areas such as risk management, internal security operations and threat response.

Q: How do Veritas solutions help agencies implement rigorous security?

The Veritas Product Security Policy meets or exceeds NIST and DISA standards and all Veritas products are built to the specifications required in the DISA Security Technical Implementation Guides. Veritas incorporates a comprehensive process for identifying product security vulnerabilities into all of our development cycles. Additionally, Veritas conforms with U.S. Department of Defense response time requirements for remediating reported product vulnerabilities.

To learn more best practices on how to more effectively manage government data, download the handbook:
www.govtech.com/datamanagement

VERITAS™ | carahsoft.