How to Rise to the Challenges of Data Protection

Nearly every discussion about cybersecurity eventually arrives at a common point: **How do you protect the data?** This focus is especially important as agencies undertake modernization efforts. Increasingly, modernization initiatives involve extending the enterprise beyond the data center — to the cloud, to field operations or to remote workers — which introduces new risk to the data.

In a recent GovLoop roundtable, sponsored by Pure Storage and Rancher Government Solutions, government and industry experts discussed strategies for leveling up data protection strategies. Here are highlights of their discussion.

ROUNDTABLE PARTICIPANTS

Hemant Baidwan
Chief Information Security Officer, Department of Homeland Security (via separate interview)

Rajeev Raghavan
Special Counsel to the Director of the FBI

Brian Shimkaveg
Senior Director for Department of Defense/ Intelligence Community Sales, Rancher Government Solutions

Nicole Willis
Deputy Chief Information Officer, National Archives and Records Administration (NARA)

Nathan Wood
Leader, Cloud Native Architects, Pure Storage

A Tough Starting Point

Agencies face numerous challenges around data protection, some they can control and some they can't. Key concerns include:

TECHNICAL DEBT

Faced with constrained or uncertain budgets, agencies must balance keeping some legacy systems running as they modernize others. At NARA, security is a top priority of modernization initiatives, Nicole Willis said.

"We are modernizing a good number of applications and using that as an opportunity to build mature cybersecurity," she said. Likewise, in upgrading its network infrastructure, the agency is looking to strengthen its identity and access management.

HIDDEN RISKS

Although technical debt can be a challenge, at least it's a known challenge, said Hemant Baidwan of DHS. You know where the risks are, and you can factor that into your modernization initiatives. "What keeps me up at night is, are there risks I don't know?" he said.

One big challenge in large organizations is shadow IT, which is technology that employees use without proper authorization. Unvetted technology can introduce vulnerabilities into the IT environment that go unaddressed until problems arise. A related challenge is software supply chain security, Baidwan said. (See discussion below.)

OPERATIONAL COMPLEXITY

Data protection was challenging enough when everything was stored in the data center. Now data protection is everywhere, which supports cybersecurity efforts across the public and private sectors, said Rajeev Raghavan with the FBI.

"At the FBI, we've got a lot of networks, and lots of the [victims] we [work with] have lots of networks," Raghavan said. "They've got on-premises systems, they've got cloud systems, they've got homegrown software and [commercial software]." So, in addition to protecting their own systems, agencies also need to work with vendors to ensure the security of their products and services, he said.

DATA CONTROLS

Many agencies find managing data to be a complex undertaking, as they face external and internal threats, said Brian Shimkaveg with Rancher Government Solutions, which provides secure, open source-based, cloud-native solutions.

"How do they provide the boundaries and protection that they need to ensure that the data that they receive has the integrity that it has, that it's stored in an appropriate way, that it has access controls that are required and that they protect against data exfiltration?" he said.

NEW THREAT VECTORS

Data protection becomes even more daunting as agencies adopt cloud-native solutions. Cloud-native applications are dynamic by design, built to be portable, scalable and flexible, and they often involve an array of products and vendors — "more ecosystem-based vs. vendor architecture-based," said Nathan Wood of Pure Storage, which provides a modern data storage platform.

"You have to learn a whole new way of mitigating risk in that environment," said Wood. "You're dealing with an ecosystem of products that have to work together efficiently and effectively to provide alerting and observability, and all the things that we look for."

How to Better Prepare for a Breach

Data protection is not just about preventing a breach. It's about responding effectively when the inevitable breach happens. "We're really trying to get people to understand that ... incidents will happen, and they should be prepared to respond," Raghavan said.

An incident response plan spells out the roles and responsibilities of everyone involved in responding to an incident, both during and after, leaving no room for confusion, Raghavan said. "What people don't realize, especially if you haven't been hit yet, is that things move very, very quickly," he said.

With cyberattacks becoming more visible, you should loop in your communications and public affairs team, so that they can help you get ahead of any confusion or bad information. "When something happens, we want to make sure we're protecting the reputation of the agency and the trust of the public," Willis said.

In the past several years, the development of more robust virtual operations has improved communications and coordination activities during a response, Baidwan said. Still, agencies need a fallback system in case the virtual environment itself is compromised, he said — and they must test the backup plan as well.

What's more, the plan should lay the groundwork for the post-incident investigation, Wood added. Often, some of the most important clues lie in the activity logs that systems and devices on the network automatically generate, but in the rush to get everything back up and running, the IT team wipes out that data, he said.

"It's something you need to build into the plan and into the ethos of the organization to make sure we're gathering that information," Wood said.

There's another cultural dimension to incident response, said Shimkaveg. Many incidents result from people mistakenly clicking on a malicious link in an email. If you have a culture in which people feel safe admitting mistakes, "you can contain the problem as soon as possible," he said.

5 Ways to Strengthen Data Protection

As tough as the threat landscape might be, you can strengthen your defenses. Here's how:

1 TAP INTO CYBER INTELLIGENCE

Although some malicious actors single out specific organizations, most launch attacks widely across both the public and private sectors. That creates an opportunity for organizations to share information about what's being attacked, the methodologies being used and the damage done, Raghavan said. "There's a wealth of data in all those organizations in those sectors that needs to be highlighted, needs to be leveraged and then shared more broadly," he said.

The key is to establish those relationships with your peers in the community before an incident happens, beginning with the local FBI field office. In the event of a widespread attack, the FBI can be an invaluable source of threat intelligence, said Raghavan.

2 FOCUS ON SUPPLY CHAIN SECURITY

Most software developers build their programs around countless components from commercial vendors or open source repositories, which makes it possible to accelerate the development process. But there's a catch: Any flaws or vulnerabilities in the component parts put the larger system at risk. When vulnerabilities in a product are discovered, agencies might not know they even use that product, and so they're exposed.

"The best defense mechanism against outer attacks is to maintain that bulwark of defense by patching when you can," said Shimkaveg, whose company focuses on open source software and supply chain security. "The question is, do we have the knowledge of the integrity of all the pieces and parts, giving us confidence in the system?"

3 KNOW WHAT YOU NEED TO PROTECT

Wood describes a three-step approach to developing a data protection strategy: Know what data you need to protect, know the value of that data and build the infrastructure needed to provide the necessary protection.

The foundation of any protection strategy is redundancy, he said. Borrowing an old military adage, data storage experts like to say, "Two is one and one is none." That is, having two sets of a dataset is as good as having just one, because something is bound to go wrong with one copy, either because of human error or a malicious act. Likewise, if you have just one copy, you might as well have none.

"You need to have multiple copies of data stored in different places and protected in different ways in order to ensure you always have a valid copy," Wood said.

It's also important to understand where the data is flowing — whether it's moving to the cloud, out to the edge or even to outside partners — and where it might be vulnerable. Your protection strategy might include encrypting data both at rest and in motion, and securing the transport network of that data, he said.

4 LINK CYBER SPENDING TO OUTCOMES

Cybersecurity continues to be one of the biggest drivers for modernization. The challenge, given budget constraints, is figuring out the best way to allocate available resources.

With that in mind, DHS developed the Unified Cybersecurity Maturity Model. The framework "allows us to tie the investment dollars to the cybersecurity of a [high-priority] program and its component systems," Baidwan said.

In simple terms, the framework guides the department through the process of identifying critical cybersecurity challenges, determining the resources needed to address them, and showing how that investment qualitatively improves the overall cyber maturity of the program.

This automated risk prioritization allows for system teams to optimize time spent in remediating system deficiencies to provide the best achievable system maturity with the least time and staff expenditures.

This model has proven invaluable when talking about cyber investments not just with IT experts, but with chief financial officers, budget examiners and lawmakers. They also use the model to track and report on the outcomes of those investments, Baidwan said.

5 HAVE A LEARNING MINDSET

Finally, remember that in cybersecurity and data protection, good enough is never good enough for long.

Cybersecurity requires continuous learning, said Willis. Think about the incident response plan. As good as it might be, you need to revisit that plan after an incident and incorporate the lessons you learned. In the same vein, you need to continually assess the risks in your environment and the effectiveness of both your cyber processes and the underlying technology.

And this responsibility can't fall wholly on the IT or cyber team, Willis said. It's everybody's responsibility. "You have to make some changes in the way the organization operates, being clear on the roles and responsibilities and resources, [and] promoting that proactive culture of continuous assessment and continuous improvement," she said.

To learn more, visit Pure Storage and Rancher Government Solutions.

govloop

PURESTORAGE®

RGS
Rancher Government Solutions