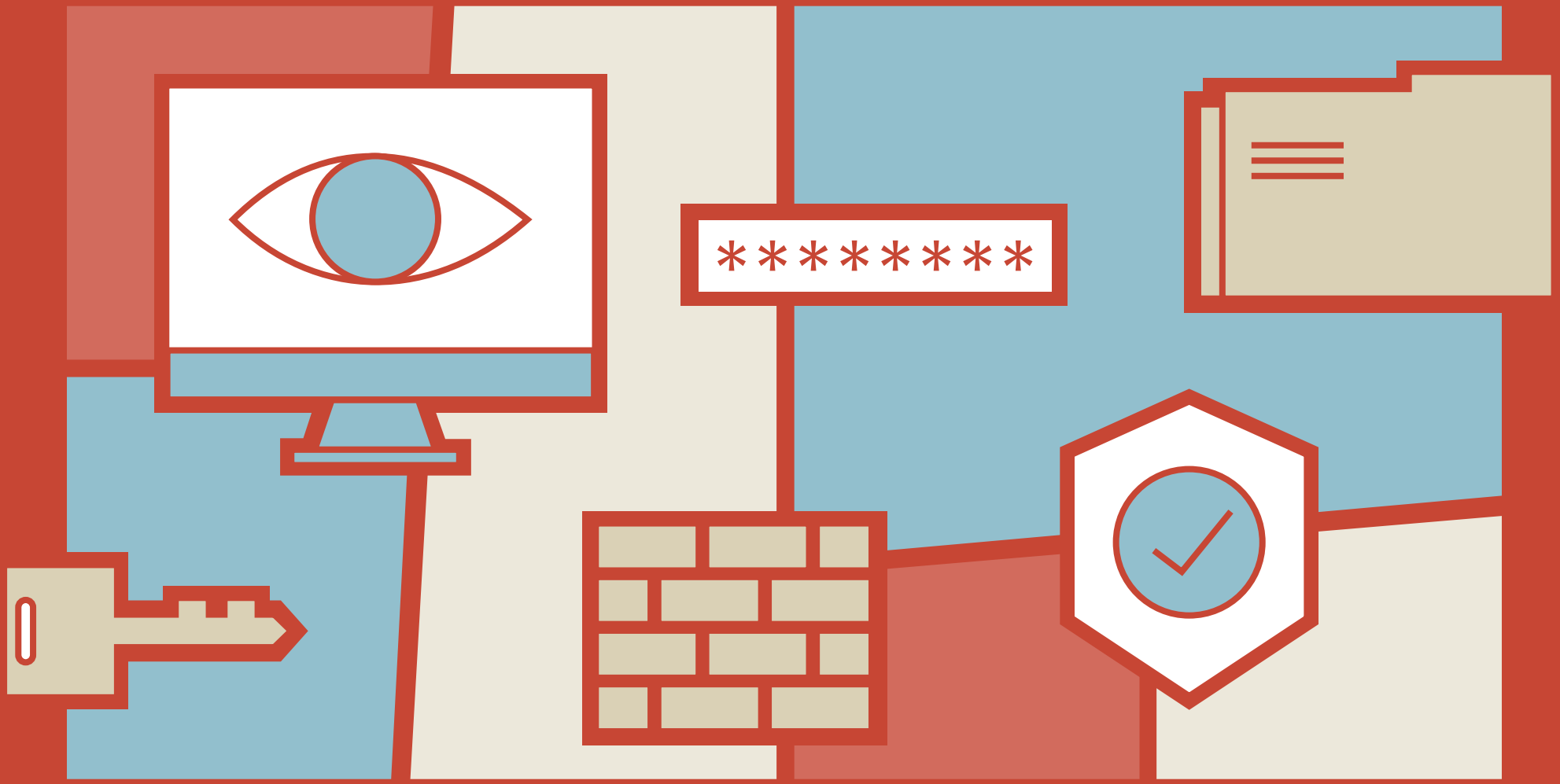
4 Steps Agencies Can Take for a Strong Cyber Foundation



govloop

ORACLE

Executive Summary

Government agencies face a tall order in improving their cybersecurity postures. The White House Executive Order on Improving the Nation's Cybersecurity from May 2021 sets clear mandates for both industry and government, including directives for agencies to modernize their approach to cybersecurity by adopting best practices, implementing zero-trust architectures and moving toward secure cloud services, among other steps.

Getting to that point, however, is no simple matter for many agencies. Despite subsequent guidance and directives from the Cybersecurity Infrastructure Security Agency (CISA), the Office of Management and Budget (OMB) and others, some agencies still struggle with the basics of cybersecurity, as the low grades a Senate committee handed out to eight critical agencies last year indicates. And the task of modernizing cybersecurity will only become more complex as agencies increase their use of the cloud.

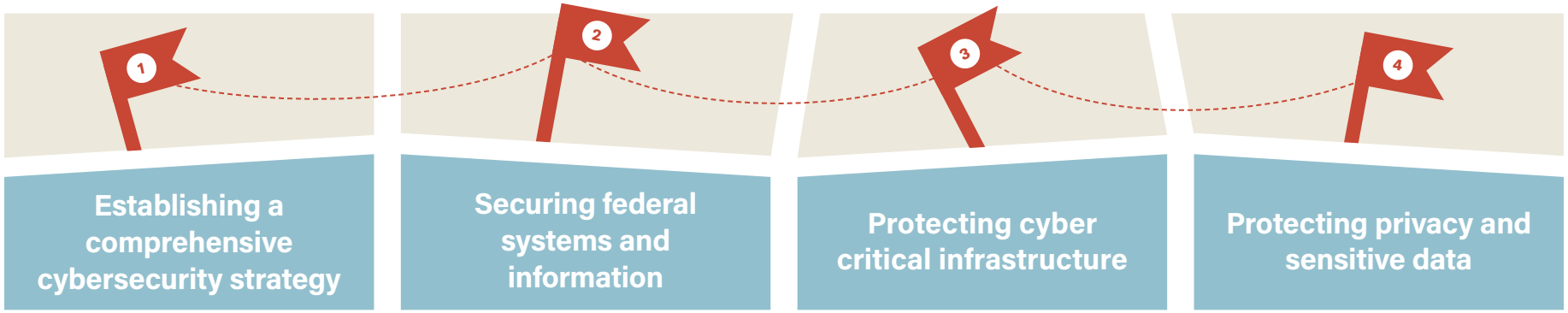
To bring their cybersecurity postures on par with the current threat landscape – and meet the mandates of the E.O. – agencies need to work from the ground up, establishing a foundation based on a clear assessment of their current posture, building a framework for moving forward and implementing a roadmap that outlines clear steps toward improvements in cloud security, detection and response, identity management and information-sharing.

To learn more about how agencies can achieve their cybersecurity goals, GovLoop partnered with Oracle for this playbook. We'll examine the challenges agencies face, the state of current cybersecurity postures and the steps they need to take to move forward, highlighting the progress one agency has made so far.

Need to Know

4 Top Challenges

Major challenges faced by federal agencies, as identified by the Government Accountability Office (GAO):



Source: GAO

Feds Say Cloud Complicates Security

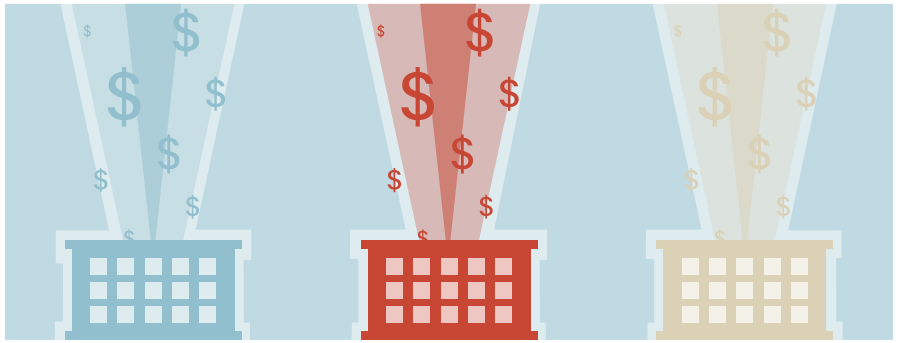
More than three in four government IT decision-makers (**78%**) rate migrating and managing data from legacy systems to the cloud as very or somewhat challenging for their agency.

50% of government IT decision-makers say their agency is using a mix of security tools for on-premises and cloud threats, creating a gap in visibility.

C-: the overall cybersecurity grade a Senate Homeland Security Committee gave eight critical agencies dealing with sensitive information in a 2021 report.

In the News

These are some of the steps agencies are taking to get their cybersecurity houses in order.



TMF Investing in Agencies' Cyber Improvements

The federal Technology Modernization Fund, which to date has invested more than $500 million in helping agencies modernize IT and improve cybersecurity, recently announced new investments in the Department of Labor, AmeriCorps and the U.S. Agency for International Development (USAID).

A $5.6 million investment in USAID, for example, focuses on improving security controls across its vast and distributed network. "TMF funding will allow USAID to accelerate its zero-trust initiative across an 'anytime-anywhere' organization of over 13,000 end users worldwide," said Paloma Adams-Allen, the agency's Deputy Administrator for Management and Resources.

OMB Gives Zero Trust Priority, Focuses on Shared Defense

An Office of Management and Budget memorandum in July on the administration's cross-agency cyber investment priorities gives precedence to implementing zero-trust strategies, along with IT modernization.

The memo requires agencies to achieve specific goals detailed in the Federal Zero-Trust Strategy by the end of fiscal 2024. A cross-government team of cybersecurity experts from OMB's Office of the National Cyber Director and CISA is working with agencies on achieving those goals.

The objectives OMB is focusing on include the adoption of secure cloud services and several steps involving a shared defense. The memo calls for developing and deploying shared federal products, services and standards; using shared security technologies, such as DHS's Continuous Diagnostics and Mitigation program; and sharing threat information and awareness among security and IT operations teams across the federal enterprise.

How Agencies Can Get Their Cybersecurity Houses in Order

In addition to compliance requirements and mandates from the White House, agencies have very good reasons to bolster their cybersecurity. Most important among them is that the threat is real and growing.

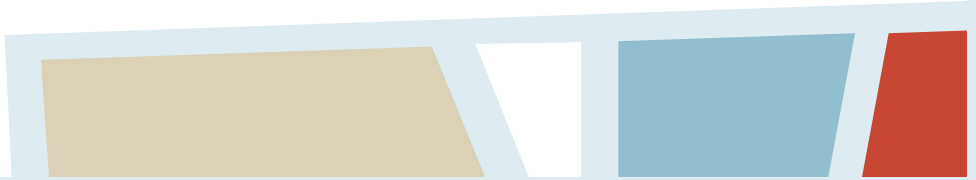
Notable attacks such as the SolarWinds supply-chain attack, which affected government, industry and academia, or the Colonial Pipeline infrastructure attack, which shut down a major U.S. oil pipeline, have drawn a lot of attention, but attacks overall are becoming more frequent and targeted. A study by Check Point Research found 1,136 cyberattacks per week in the government/military sector in 2021, a 47% increase over the year before.

The highly distributed cloud computing environment has expanded the attack surface for agencies by, among other things, increasing the number of users with access to systems, including remote users. In addition to human users, cloud services and the Internet of Things have exponentially increased the number of network identities, which include bots, application programming interfaces and Internet-of-Things devices.

"A lot of things have changed in the last three to four years, and that is exactly why the executive order is timely," said Jackson Thomas, Managing Director of Cloud Infrastructure for Oracle.

"Even before the pandemic, there was a greater push to move workloads and applications to the cloud," he said. "And the reality is that more than 90% of the customers out there, government and commercial, have their deployments staggered between on-premise, private cloud, public cloud and so forth. So the whole notion of a closed perimeter is long gone."

Here is a look at four essential steps that can help agencies secure data and applications in that environment.



1

Perform a Thorough Cyber Assessment

Agencies need to know where they stand before they can move forward. And that requires a thorough assessment of cybersecurity capabilities in their enterprises.

"Having a 360-degree view of your security posture, regardless of where your application is running, is extremely important," Thomas said. "Just because your applications and data are in the cloud does not mean [they are] 100% secure."

The cloud itself is secure, he said, because cloud service providers (CSPs) have made security a priority, but agencies have their own parts to play as the data custodians in a shared responsibility model. "The data ownership still lies with the customer, and they're responsible for the security," he said.

Agency security teams could start with self-assessments such as the worksheet developed by Oracle and GovLoop for assessing agency progress in five areas:

1. **Cybersecurity**, to assess agency implementation of least-privilege access policies and multifactor authentication (MFA)
2. **Data security**, to establish whether data is always encrypted in transit and at rest, and whether the agency's CSP has access to content, can help find and protect sensitive data, and provides fully redundant storage
3. **Compliance**, to determine whether the cloud vendor meets the requirements of the Federal Risk and Authorization Management Program (FedRAMP) and other federal, state, local and international standards
4. **System security**, to establish the physical data center protections (backup power, video surveillance) and cyber support (automated patching, penetration testing and vulnerability assessments) provided by the CSP
5. **Infrastructure security**, to assess whether the agency's hypervisor is built for cloud security, and whether the CSP practices isolated network virtualization

Meanwhile, technology- and security-focused agencies also provide guidance and, in some cases, direct assistance. NIST's Cybersecurity Framework, for example, also provides a source of workshops and use cases of what other agencies are doing. CISA also will perform risk and vulnerability assessments to help agencies identify weaknesses that need to be addressed.

2

Adopt a Framework

Once agencies have assessed their security posture and prioritized their risks, they must develop a framework based on a model of detect, protect, respond and recover – which is spelled out as part of NIST's Cybersecurity Framework.

A solid framework can bring consistency across the enterprise, something many organizations are lacking. "There are multiple issues with the way cybersecurity is adopted today," Thomas said. "Whether it is in the identity and access management space or in basic cybersecurity principles like encrypting, it is not consistent across the deployment environments."

Consistency is key because of the varied environments agencies manage, even if it's all in the cloud. "Not all cloud is made equal," Thomas said, noting the differences between private, public and hybrid clouds. Even within public clouds, whether a cloud is first generation or the more secure second generation, such as Oracle's Gen 2 Cloud, makes a difference.

Security is further complicated by evolving cloud-native technologies such as containers, serverless computing, infrastructure as code (IaC) and edge computing, all of which can present new security risks. All of this also contributes to the identity sprawl – both human and non-human – across the enterprise.

A framework for cybersecurity needs to include strong identity management within a zero-trust architecture (ZTA), making use of practices such as multifactor authentication, network segmentation, continuous monitoring and other measures. And it should cover how an agency responds to and recovers from attacks, as well as detecting and protecting against them.

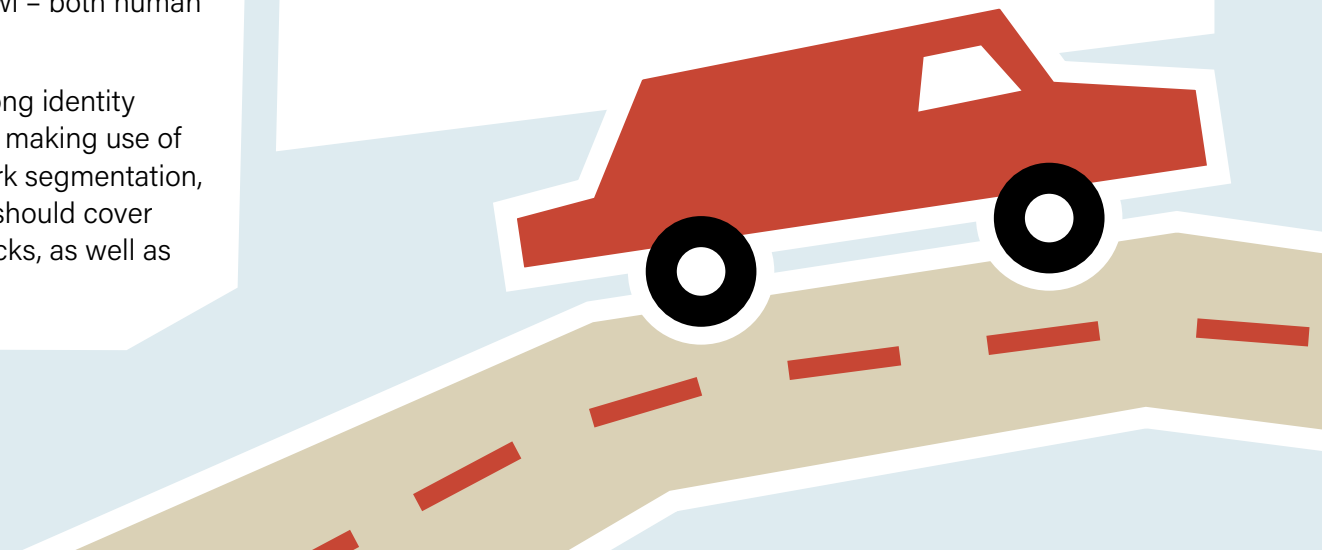
3

Build a Roadmap

Working from their assessment and framework, agencies can now go about implementing improvements to cloud security, ID management, detection and response capabilities, as well as information-sharing.

As much as possible, however, it helps to have improvements built in by the cloud provider. Although there is a definite place for security services that are "bolted on" by a third-party provider, such as in a multi-cloud environment, built-in technology offers deeper integration with the provider's infrastructure and can provide a simpler, more cost-effective way to make improvements without overtaxing the IT staff – security services need only to be turned on, rather than integrated. Cloud providers such as Oracle also provide a built-in framework for identity and access management.

In multi-cloud environments, agencies also can reduce the ops team's workload through the type of cloud services they use. When possible, choose Software as a Service (SaaS), which puts the fewest operational demands on the agency, then Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) only when SaaS and PaaS aren't a fit. Even then, automated tools such as Terraform can help lessen the complexity.



4

Add Cyber Capabilities

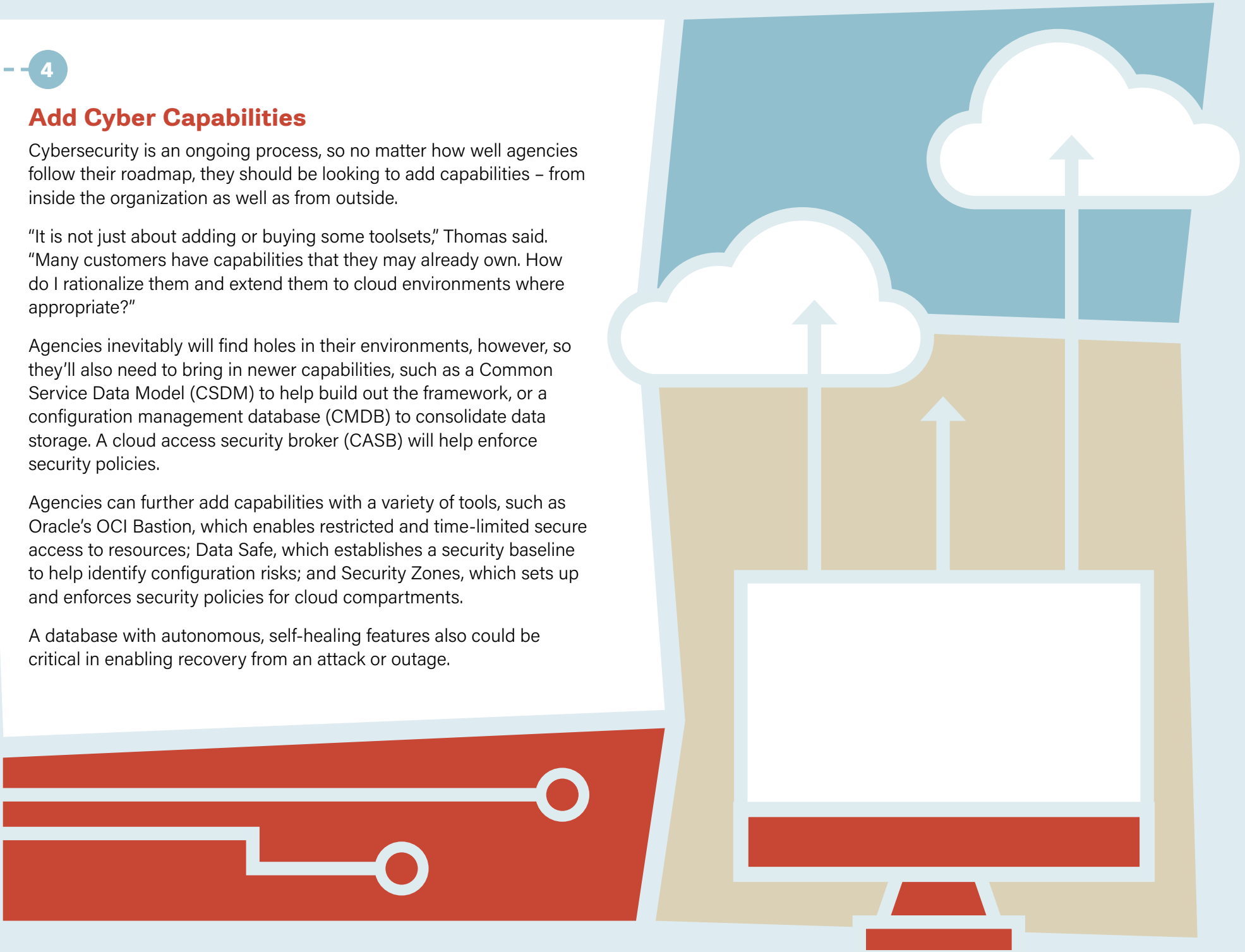
Cybersecurity is an ongoing process, so no matter how well agencies follow their roadmap, they should be looking to add capabilities – from inside the organization as well as from outside.

"It is not just about adding or buying some toolsets," Thomas said. "Many customers have capabilities that they may already own. How do I rationalize them and extend them to cloud environments where appropriate?"

Agencies inevitably will find holes in their environments, however, so they'll also need to bring in newer capabilities, such as a Common Service Data Model (CSDM) to help build out the framework, or a configuration management database (CMDB) to consolidate data storage. A cloud access security broker (CASB) will help enforce security policies.

Agencies can further add capabilities with a variety of tools, such as Oracle's OCI Bastion, which enables restricted and time-limited secure access to resources; Data Safe, which establishes a security baseline to help identify configuration risks; and Security Zones, which sets up and enforces security policies for cloud compartments.

A database with autonomous, self-healing features also could be critical in enabling recovery from an attack or outage.



How Cloud Security Is a Shared Responsibility

A common source of confusion in securing cloud infrastructures is the role agencies have in the Shared Responsibility Model, which defines the security responsibilities of cloud providers and their customers.

In general terms, the provider is responsible for the security of the cloud itself and the hardware and software that goes into it. Agencies are responsible for what they have in the cloud, including their data, applications, operation systems, and identity and access management controls.

But agency responsibilities can vary depending, for example, on the type of cloud service they're using. A study by Oracle and KPMG found that confusion over customer responsibilities can result in misconfigurations and other errors with serious consequences, including data loss, malware and stolen credentials. So it's essential that agencies fully understand their role in cloud security.

"We consume services from cloud in three broad categories: infrastructure as a service, platform as a service and, the highest layer, software as a service," Thomas said. "Depending upon what service you are consuming, your responsibility from a security perspective drastically changes."

Here's how it typically works:

- With **IaaS**, the cloud service provider is responsible for the cloud infrastructure, and the agency holds responsibility for everything from the operating system on up, including data and applications.
- With **PaaS**, which can include a managed middleware service like databases, the CSP will be responsible for the operating systems and the middleware, in addition to the infrastructure, while the agency is responsible for the data and managed services.
- With **SaaS**, the CSP is responsible for the infrastructure, the OS, the middleware and application, but not for the application configurations, the data and the account itself, which are the agency's responsibility.

Essentially, as you move from IaaS to SaaS, the agency's areas of responsibility decrease, but they still are responsible at least for data – the most important resource it owns – as well as the processes performed with that data. And although the provider takes a larger share of responsibility with SaaS, Oracle's study found that the shared model for securing SaaS was the most confusing for customers.

Adopting a Responsibility Matrix

Agencies could benefit by adopting a cloud security responsibility matrix that delineates the CSP and agency responsibilities for each type of cloud service. The General Services Administration's Cloud Information Center offers an illustrative matrix covering legacy IT, IaaS, PaaS and SaaS, along with guidance on security controls and the Federal Information Security Management Act (FISMA) mandates on agency responsibilities.

Regardless of the type of cloud services being consumed and the agency's relative share of responsibilities, meeting those responsibilities is crucial. Maintaining the data, applications and configurations puts agencies in control of their most vital assets, which must be secured.

"Having a basic understanding of who owns what from a security perspective, as you consume these services, is extremely important," Thomas said. "Just because you're consuming cloud, assuming everything is owned by the cloud provider is a wrong assumption to make."

ORACLE CLOUD

Learn how Oracle Cloud can help increase speed and capabilities while lowering costs

Visit Oracle.com/Federal

Conclusion

The White House Executive Order puts something of a burden on agencies to meet a strict set of mandates, but it also puts the realities of cybersecurity in a growing and increasingly complex cloud environment into sharper focus. Adopting cybersecurity best practices – from MFA and zero trust to building in resiliency – is necessary to protect agency data and systems, and ultimately, perform agency missions.

"The E.O. helps put things into perspective: the challenges in the space, and what measures government and commercial entities can take to secure the data and applications," Thomas said. "The problem is going to get more complex as we move forward."

Looking ahead, agencies will need to make greater use of advanced technologies such as artificial intelligence and machine learning, which will provide the advanced analytics and automated machine-to-machine processes necessary to maintain security. "Using machines to do most of the work is going to be critical," Thomas said.

Government Resources

Guidance, tools and, in some cases, direct assistance are available to government agencies.

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework webpage includes guidance on implementing the framework, examples of what some agencies are doing, regular updates on new guidance and links to workshops.

In addition to offering guidance documents, CISA will conduct risk and vulnerability assessments – upon request and as resources are available – at federal agencies, private organizations and state, local, tribal and territorial governments that identify vulnerabilities that adversaries could potentially exploit to compromise security controls.

CISA also will help organizations use NIST's Cybersecurity Framework to improve their cyber resilience.

And CISA's Cybersecurity Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment of an organization's operational resilience and cybersecurity practices. Conducted as a self-assessment or as an on-site assessment facilitated by Department of Homeland Security cybersecurity professionals, the CRR assesses enterprise programs and practices across 10 domains including risk management, incident management and service continuity.

Zero-Trust Guidance

- OMB's federal strategy on moving to a zero-trust architecture
- The National Security Agency guidance on embracing a zero-trust security model
- CISA's Zero-Trust Maturity Model

Supply Chain Security

The security of the software supply chain also is a focus for government. Guidance includes:

- **OMB:** Enhancing the Security of the Software Supply Chain
- **NIST:** Software Security in Supply Chains

Thank you to Oracle for their support of this valuable resource for public sector professionals.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.
www.govloop.com | @GovLoop