

# 6 Ways to Reduce Data Breach Risk



# Introduction

Cyberattacks are inevitable, and when they happen, the effects are often costly and long-lasting. This is especially true with data breaches because they can affect many people and damage the already fragile trust between an agency and constituents. Although government entities can't eliminate their risk, they can reduce it.

The actual process of reducing risk, however, poses challenges as well. Data volume continues to rise. And most agencies' IT environments are complex — making it critical for IT managers to understand what data they need to protect, where it's stored and how it moves among users, agencies and systems.

Standards from the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) help, but agencies must also have in place trained staff, a solid governance structure and visibility of their surface area.

In this report, we look at specific steps agencies can take to reduce risk. The content is drawn from a recent GovLoop virtual event. To view the full event, [click here](#).



# 6 Steps to Take

During a GovLoop online training on Sept. 28, 2022, three industry experts provided six approaches for reducing risk. These approaches are a starting point — the steps and their components will change along with technological and threat evolution. “It’s an ongoing battle,” said Lester Godsey, Chief Information Security Officer for Maricopa County, Arizona.



# 1

## Take inventory.

When it comes to cybersecurity, you can’t protect what you don’t know exists. “How can you legitimately determine what the risk is to the enterprise if you don’t know what’s in it?” Godsey said. “Inventory is the starting point of everything else that we do.”

While the concept of inventory has existed for decades from an IT perspective, it’s important to note that the definition of what an asset is needs to expand to include:

- **Data**
- **Cloud providers**
- **The companies cloud providers depend on**

An expansive view of your environment ensures your agency is accounting for all of its moving parts, giving you a solid foundation to protect anything that’s considered a prime target for bad actors.



# 2

## Assess everything.

Besides taking note of what's in your environment, understanding how you're protecting your environment is critical. Agencies that assess their processes and policies against a leading security framework (such as NIST's Cybersecurity Framework or the ISO 27001 family of standards) are better-equipped to guard against threats.



“You have to have a starting point and understand what your current reality is with respect to: What are you doing well and what are you doing that needs to be addressed? This helps you prioritize properly based off of risk — the likelihood of an event occurring versus what the impact of said event would be on the organization.”

- Lester Godsey, Maricopa County





# 3

## Understand the role of identity.

Nefarious actors' sophistication may be increasing, but one way they access IT systems and assets is simple: through identity theft.

Because identity doesn't just refer to individuals, meaning end-user logins and passwords, the definition of identity must expand to include devices, applications and service identity.

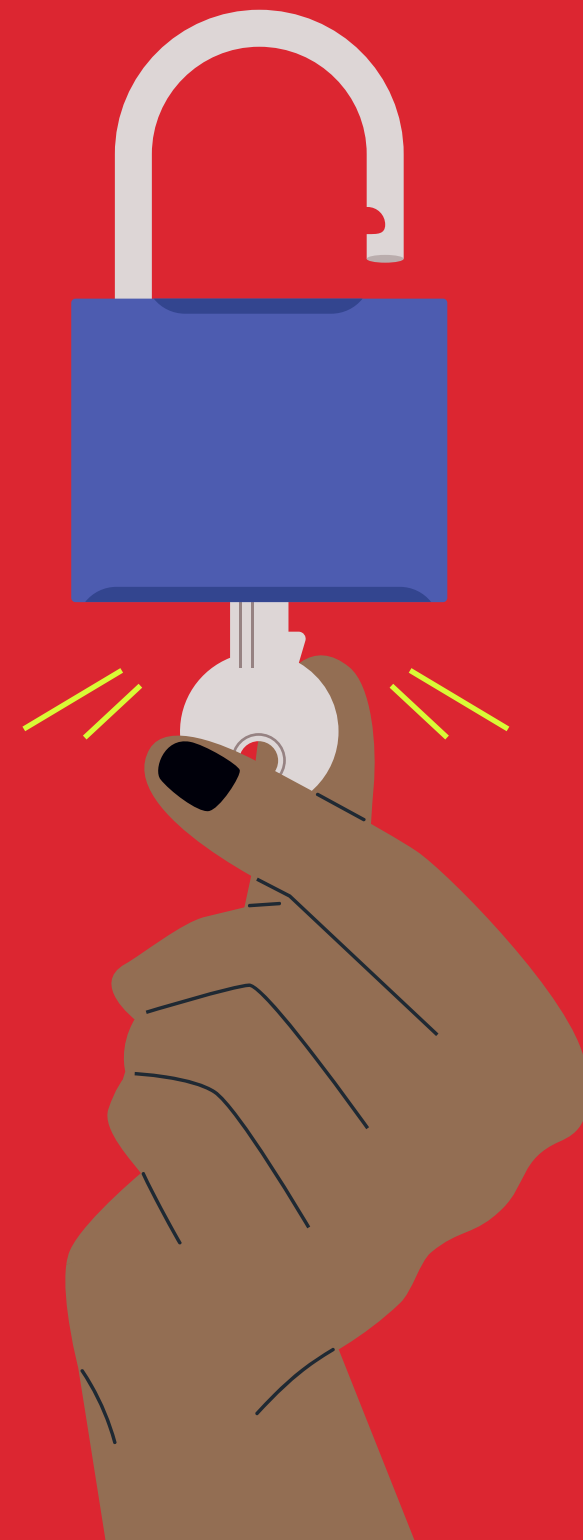
"Implementing zero trust, least privilege and multifactor authentication can significantly increase protection against this type of threat," said Carmen Taglienti, Insight Public Sector's Principal Architect for Data and Artificial Intelligence. "Between every barrier within your environment, you assume no trust. So you go back through the authentication mechanism all over again."

# 4

## Encrypt data and guard keys.

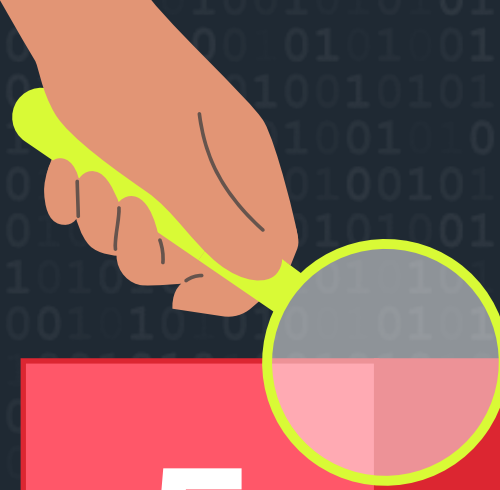
Encryption is a tried-and-true protection tactic, but understanding the level of encryption needed based on the type of asset you want to protect is critical. This is because there is processing overhead associated with how long it takes to encrypt and decrypt if accessing or processing data.

But encryption alone is not enough. Agencies must also protect the keys that decrypt because “if they become accessible, all bets are off,” said Taglienti. His recommendation? Key cycling, or frequently changing keys so that even if they’re compromised, data will remain safe.



“[Auditing] is a critical piece to reducing your risk of a data breach.”

— Matthew Lamb, Manager, State Local and Education Sales at Palo Alto Networks’ Prisma Cloud Solutions Architects

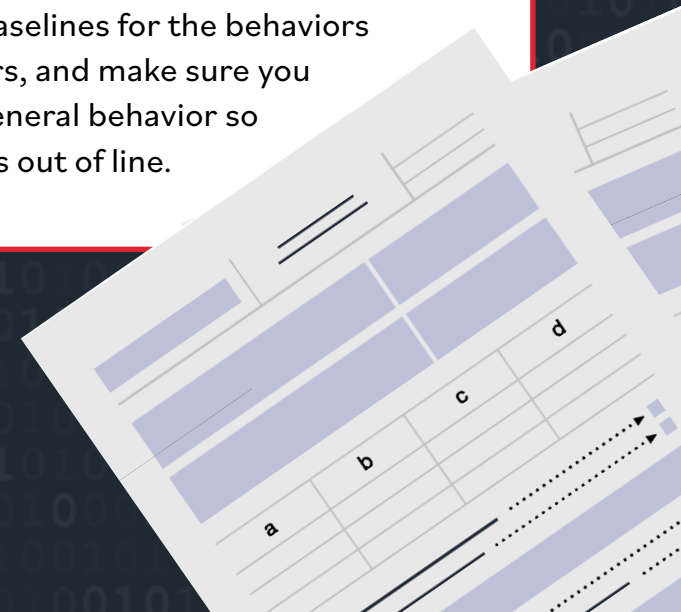


5

**Audit.**

To drive lasting success, agencies should look at their data protection strategies through a business continuity lens — and that means regular auditing. Auditing goes hand in hand with any assessments because it keeps agencies accountable to maintaining measures that are in place.

Audit strategically by setting baselines for the behaviors expected of authenticated users, and make sure you can observe them. Know the general behavior so you can identify anything that is out of line.



# 6

## Empower People.

It's long been said that people are the weakest link in the cybersecurity chain. And although training and education has increased and improved, email is still the biggest threat vector for virtually every organization, whether public or private sector.

Godsey's agency regularly conducts simulated phishing campaigns to test whether the county's 14,000 employees fall victim, and then provides training based on the results. "We are trying to create a culture to say, 'You're part of the security team at Maricopa County,'" he said.

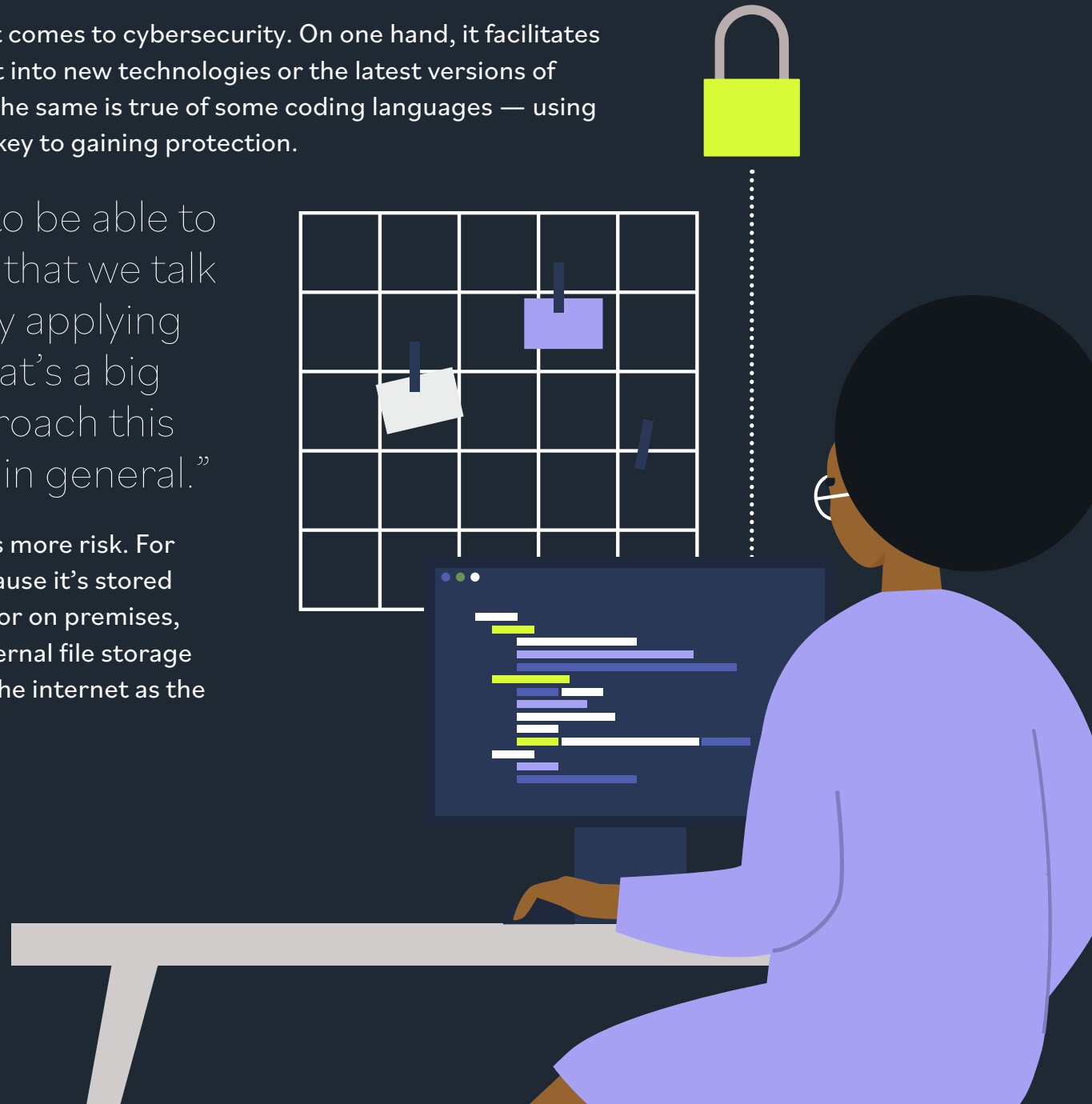


# Modernization's Role in Improving Cyber

Modernization has pros and cons when it comes to cybersecurity. On one hand, it facilitates security. For example, measures are built into new technologies or the latest versions of technologies as vulnerabilities emerge. The same is true of some coding languages — using the latest versions of those languages is key to gaining protection.

“Modernization allows us to be able to build in the best practices that we talk about rather than manually applying them,” **Taglienti said.** “That’s a big change in the way we approach this particular area or security in general.”

On the other hand, modernization brings more risk. For instance, it’s harder to manage data because it’s stored in so many locations now — in the cloud or on premises, to name a few. “We’ve now taken our internal file storage and we’ve basically used the entirety of the internet as the potential repository,” said Godsey.



# Thanks to our partners:

## AWS, Insight Public Sector and Palo Alto Networks



### About GovLoop

GovLoop's mission is to “connect government to improve government.” We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering crossgovernment 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 connect and improve government.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).

[www.govloop.com](http://www.govloop.com) | [@GovLoop](https://twitter.com/GovLoop)