10 TIPS FOR
CLOUD SECURITY

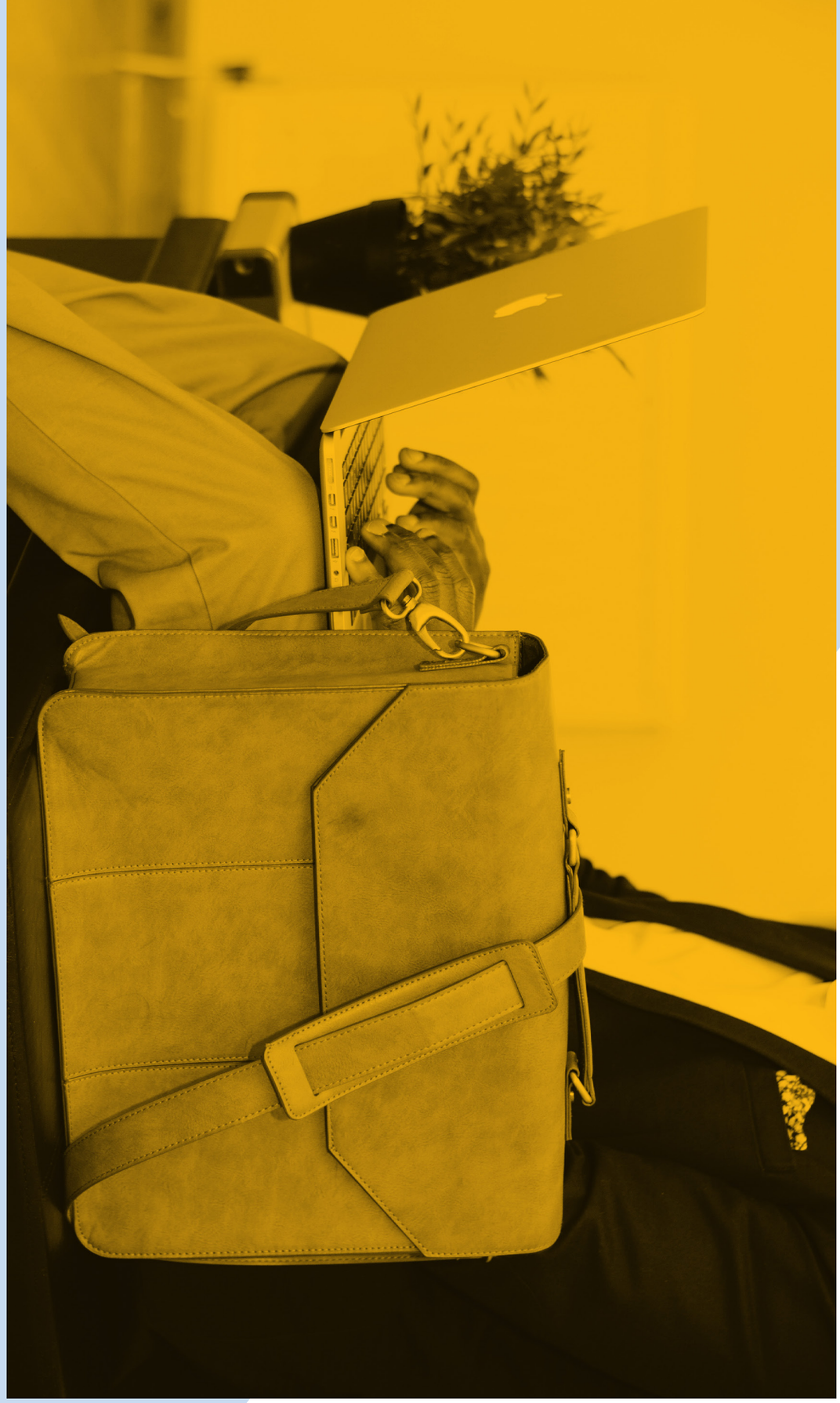
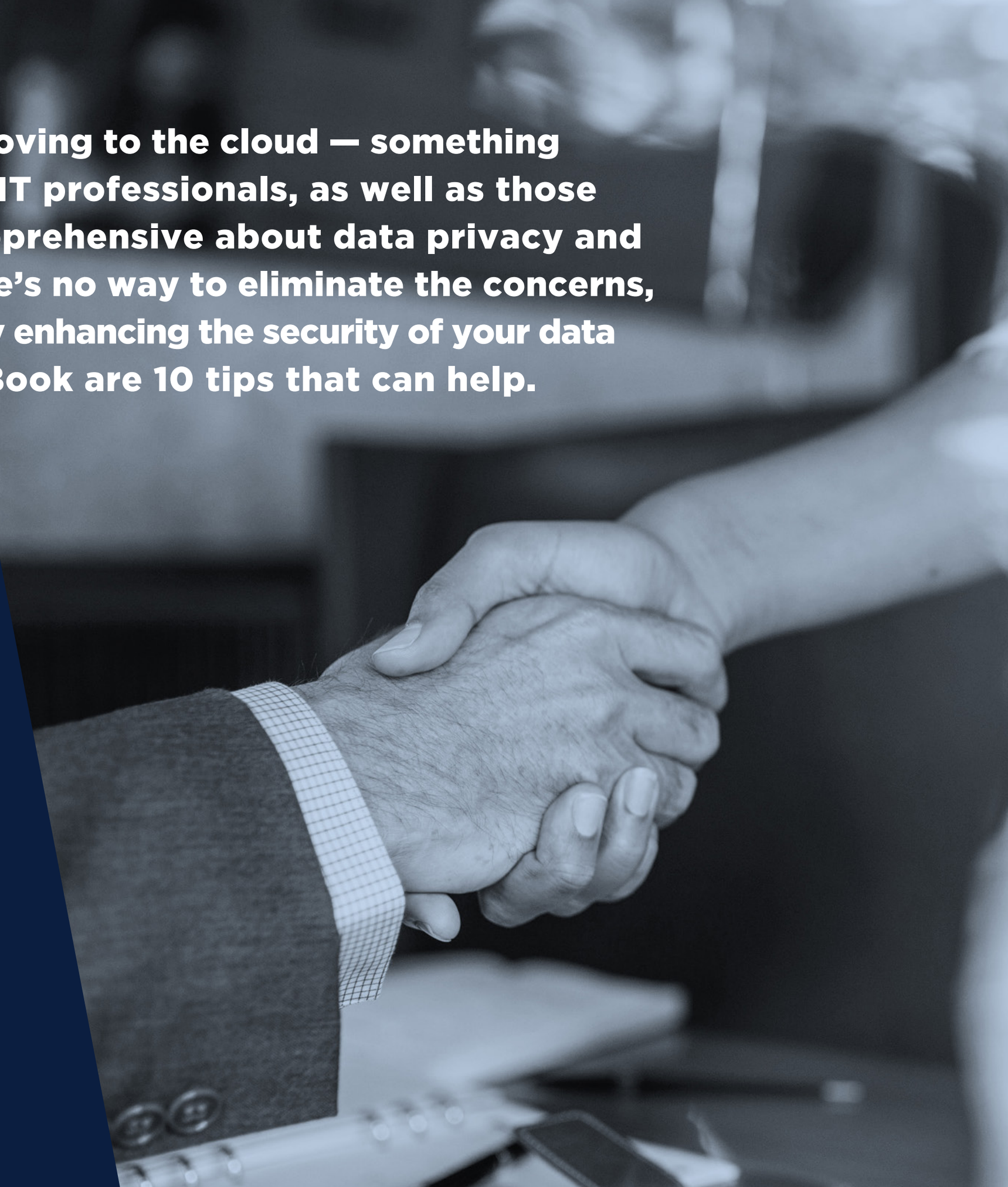


TABLE OF CONTENTS

More workloads are moving to the cloud — something that still leaves some IT professionals, as well as those in the C-suite, a bit apprehensive about data privacy and protection. While there's no way to eliminate the concerns, you can reduce them by enhancing the security of your data in the cloud. In this eBook are 10 tips that can help.



TIP 1:

KNOW YOUR DATA

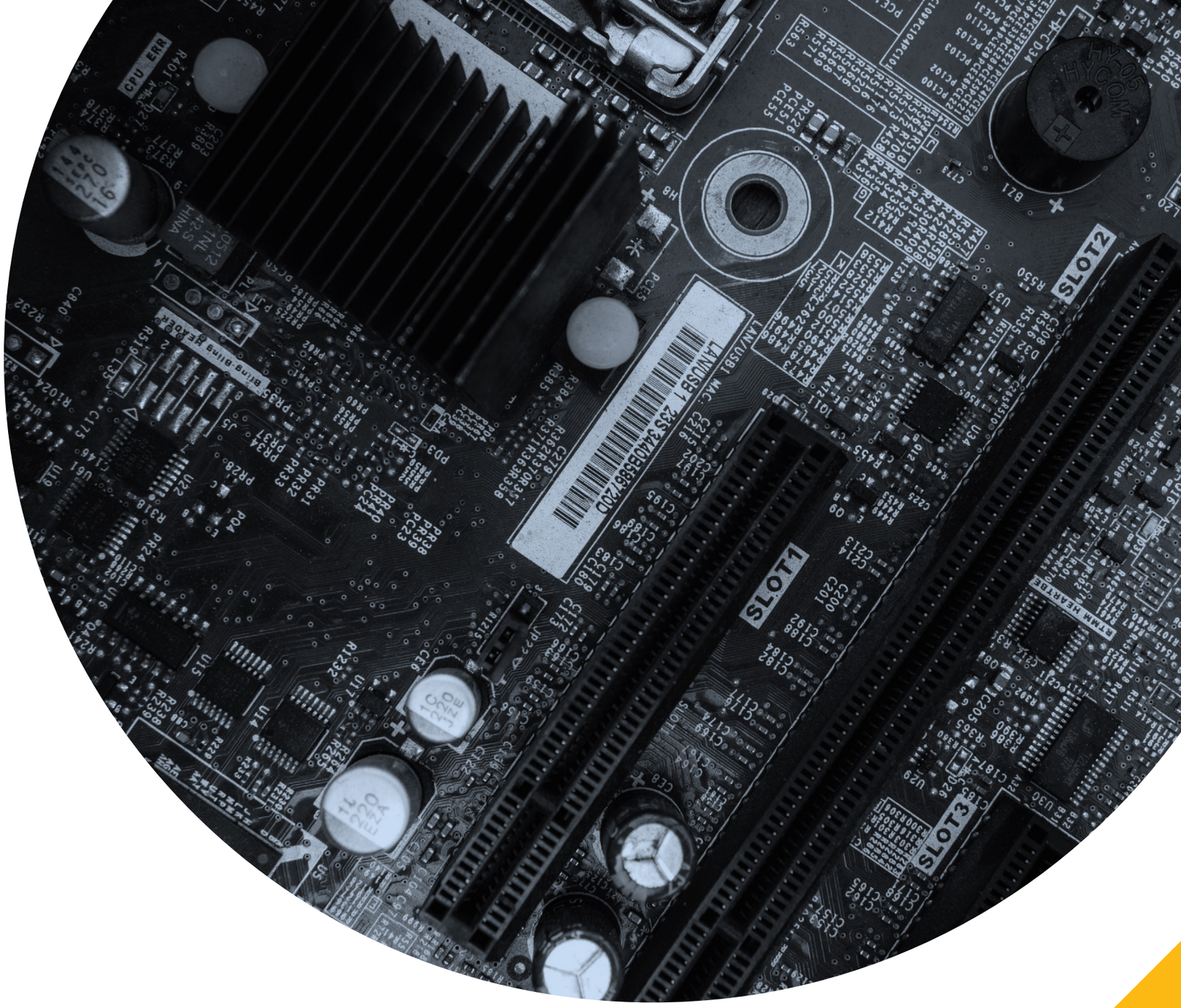
To protect your data, you must know what you have, where it is, and who has access to it.

With that information, you can then classify the data you'll be storing and/or processing in the cloud. How sensitive is it? Is it subject to privacy restrictions such as those specified by HIPAA or to standards such as PCI DSS? Does it have value as intellectual property? From there, you can define the security controls that are appropriate to protect that information. Make sure your cloud services provider (CSP) has the appropriate logical and physical controls to meet your needs — and that they are effective.

Employ two-factor or multi-factor authentication for all data that must be restricted.

You should also implement a tier structure for your access policies based on the level of trust you have for each person who can access your data.

Make sure your CSP employs identity access and authentication tools that are equal or better than what you use. For added security, supplement authentication practices with safeguards such as device or IP tracking and behavioral profiling.



TIP 2:

BEEF UP YOUR AUTHENTICATION

Protect sensitive data when it's in motion, at rest, and/or in use.

Use whole disk encryption, which ensures that all data on the disk, not just user data files, are encrypted. This can also help prevent offline attacks. All communications to host operating systems and virtual machines should also be encrypted.

Maintain an optimal security posture by retaining ownership of your encryption keys. Don't give them to your CSP.

TIP 3:

ENCRYPT AND KEEP THE KEYS

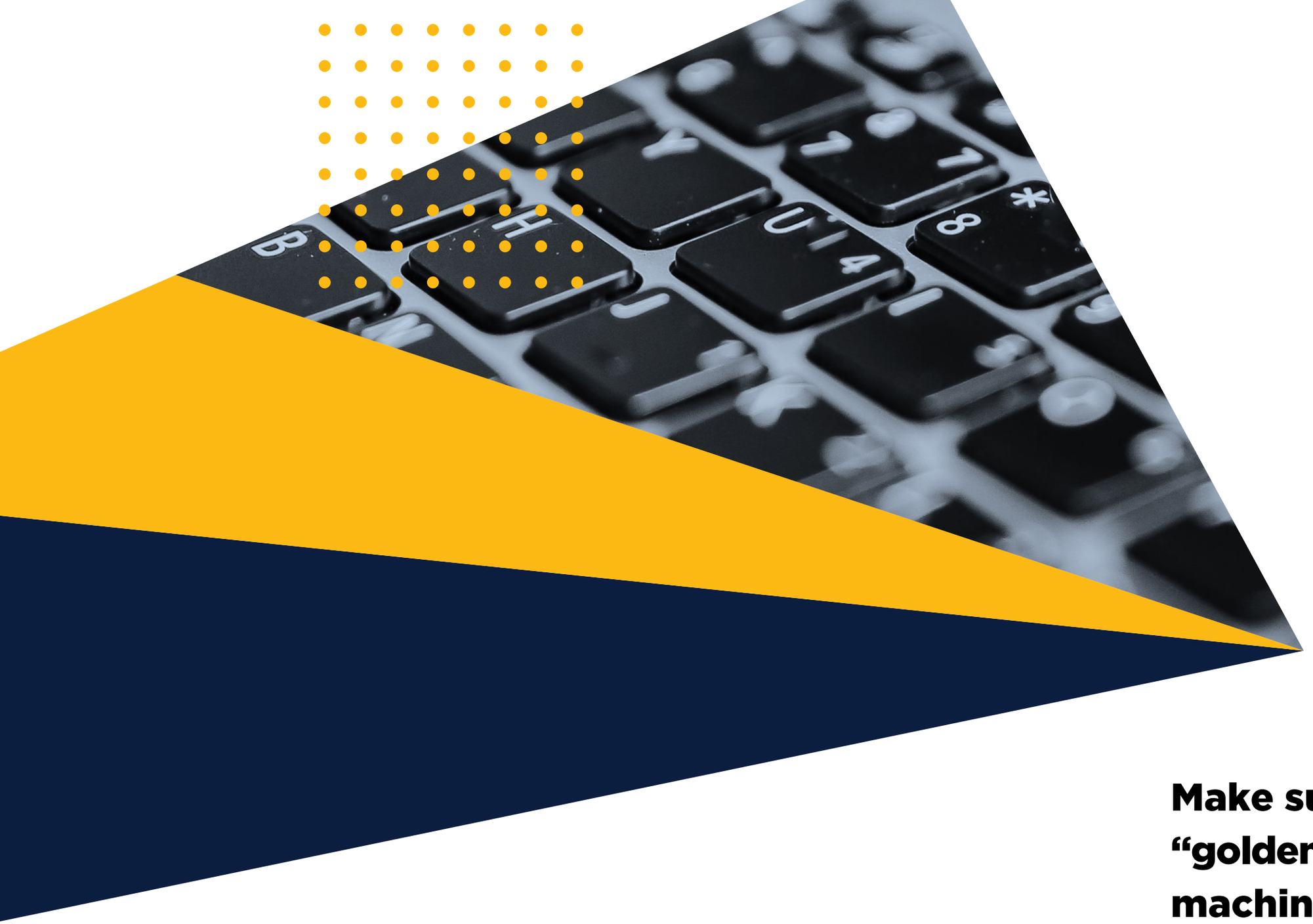
Implement comprehensive logging and reporting.

Logging is critical for incident response and forensics. Keep in mind that the reports and findings after the incident are going to depend on your logging infrastructure.

Coordinate with your CSP, and make sure performance metrics for reporting and auditing are included in your service agreement.

TIP 4:

LOG AND REPORT



TIP 5:

MAKE IT HARD

Make sure that your “golden image” virtual machines and virtual machine templates are hardened and clean.

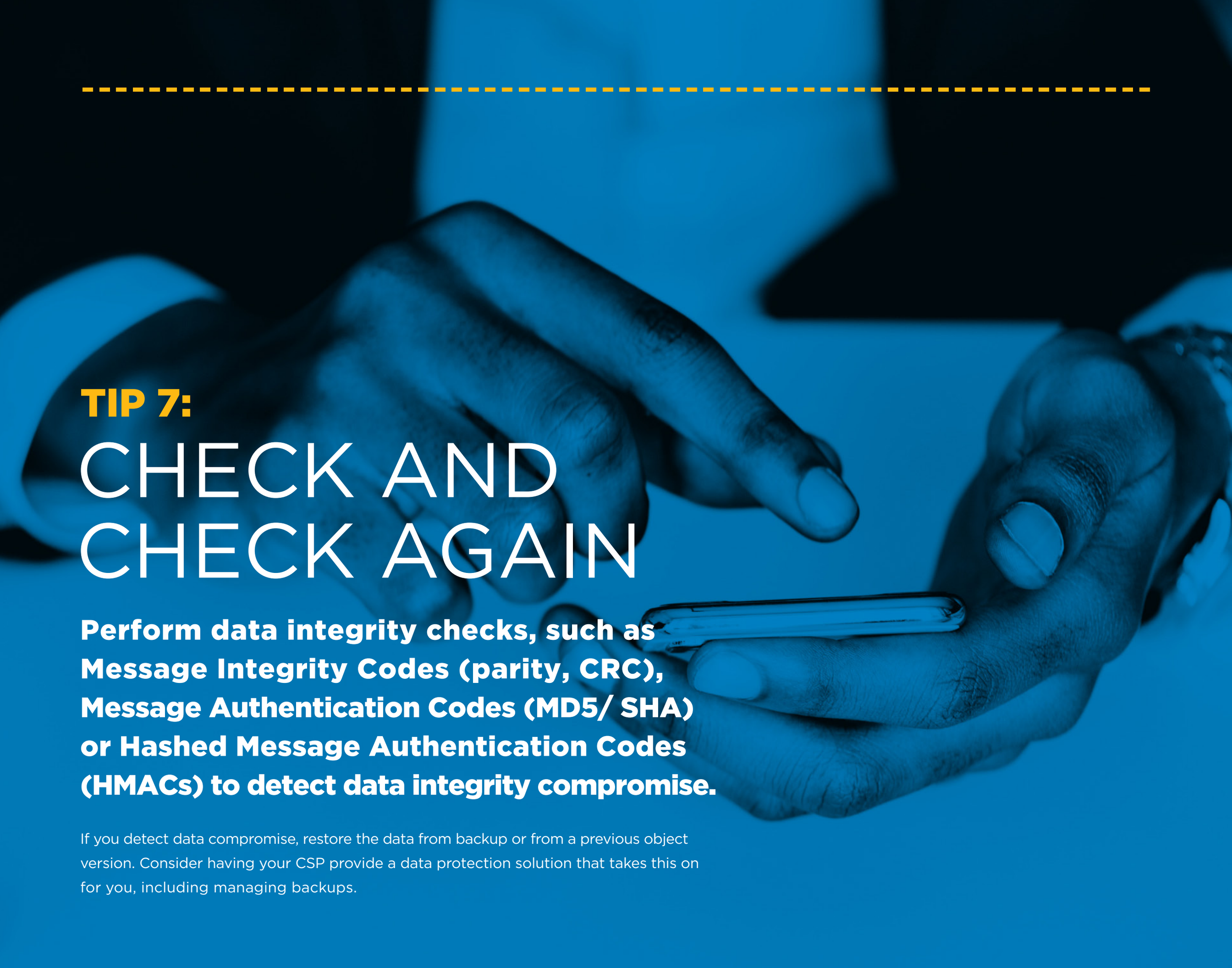
This can be done with initial system hardening when you create the images. Take advantage of technologies that enable you to update the images offline with the latest service and security updates.

TIP 6:

PLAN YOUR RESPONSE

How quickly you respond to threats and adverse events is an important component of security.

Document your responses to events and implement programs to facilitate those responses. Ask your CSP to provide you with documentation of its response plan as well.



TIP 7:

CHECK AND CHECK AGAIN

Perform data integrity checks, such as Message Integrity Codes (parity, CRC), Message Authentication Codes (MD5/ SHA) or Hashed Message Authentication Codes (HMACs) to detect data integrity compromise.

If you detect data compromise, restore the data from backup or from a previous object version. Consider having your CSP provide a data protection solution that takes this on for you, including managing backups.

Develop a playbook of the most common “insider” threats along with a checklist for actions to take.

Continuously analyze the risks of every interaction between users and networks, endpoints, applications, data and even other users.

Also make sure to implement frequent employee training and follow up on IT security. Include best practices for computer and mobile device usage, in addition to information on your organization’s security policies.

TIP 8:

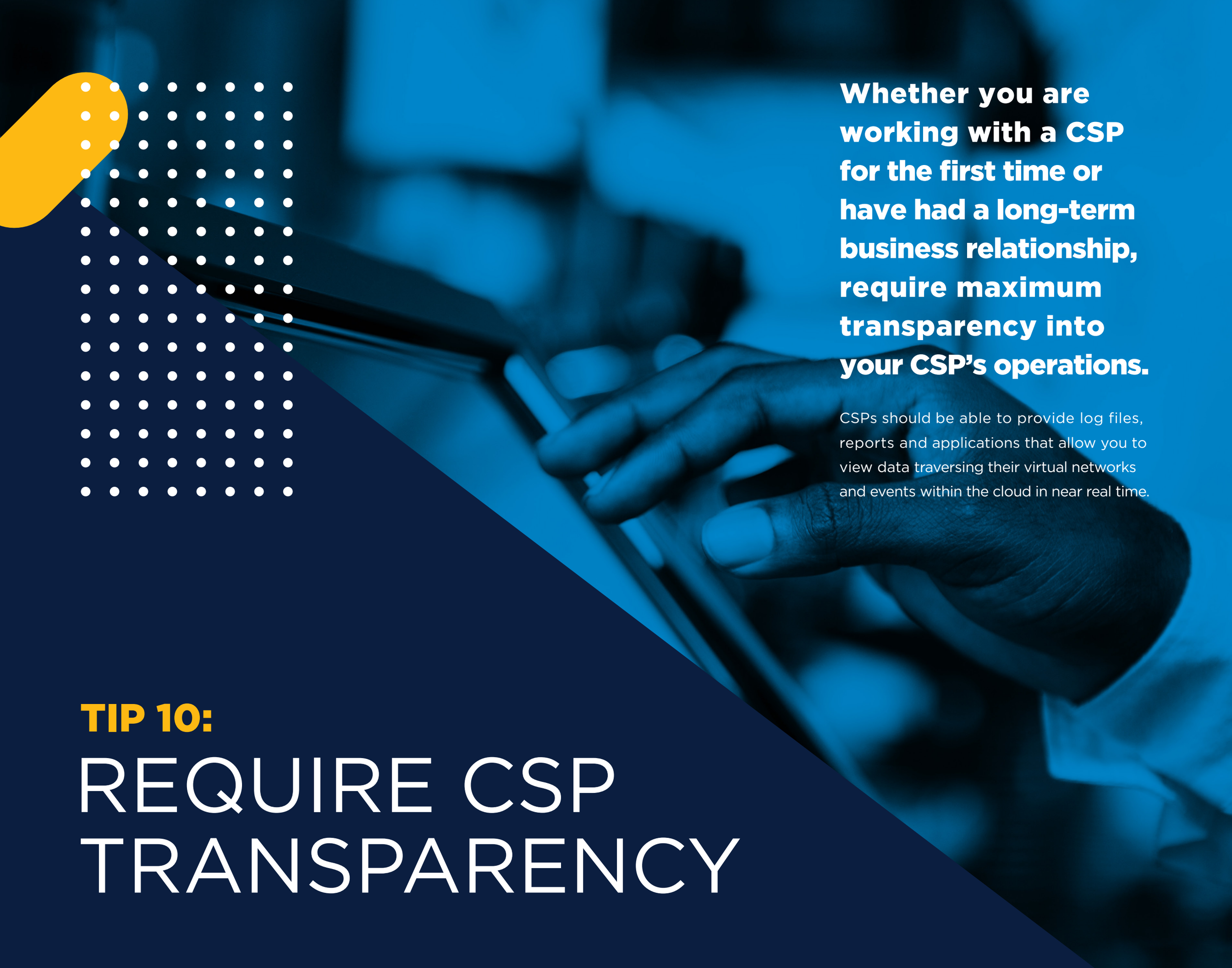
LOOK INSIDE

TIP 9:

GO OUTSIDE

While you may not want to outsource your entire IT security strategy, you can bolster it with managed security solutions from your CSP or another service provider.

Managed security services enable you to take advantage of the leading-edge security technologies and specialized security expertise that outside firms can offer—and without any upfront capital investment.



Whether you are working with a CSP for the first time or have had a long-term business relationship, require maximum transparency into your CSP's operations.

CSPs should be able to provide log files, reports and applications that allow you to view data traversing their virtual networks and events within the cloud in near real time.

TIP 10:

REQUIRE CSP TRANSPARENCY

THE US SIGNAL

CLOUD SECURITY ADVANTAGE

The CSP you choose to work with can also affect the robustness of your cloud security—and your peace of mind. That's why you may want to consider US Signal.

Powered by our wholly owned, secure fiber network and PCI- and HIPAA-compliant infrastructure, our cloud solutions are designed to prevent data loss and corruption via multiple levels of built-in security that extend to the edge. Any issues that do arise will be quickly handled before they become problems by 24/7/365 Technical Operations Center (TOC).

You can also leverage US Signal's depth and breadth of security expertise and managed security services. You'll get peace of mind knowing your data and applications are safe and that you can keep your business up and running no matter what cyber-attackers throw your way.

For more information, call us at 866.2. SIGNAL or email: info@ussignal.com

US SIGNAL®