US SIGNAL

10 TIPS FOR CLOUD SECURITY

TABLE OF CONTENTS

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.

TIP 3:

ENCRYPT AND KEEP THE KEYS

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.

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.

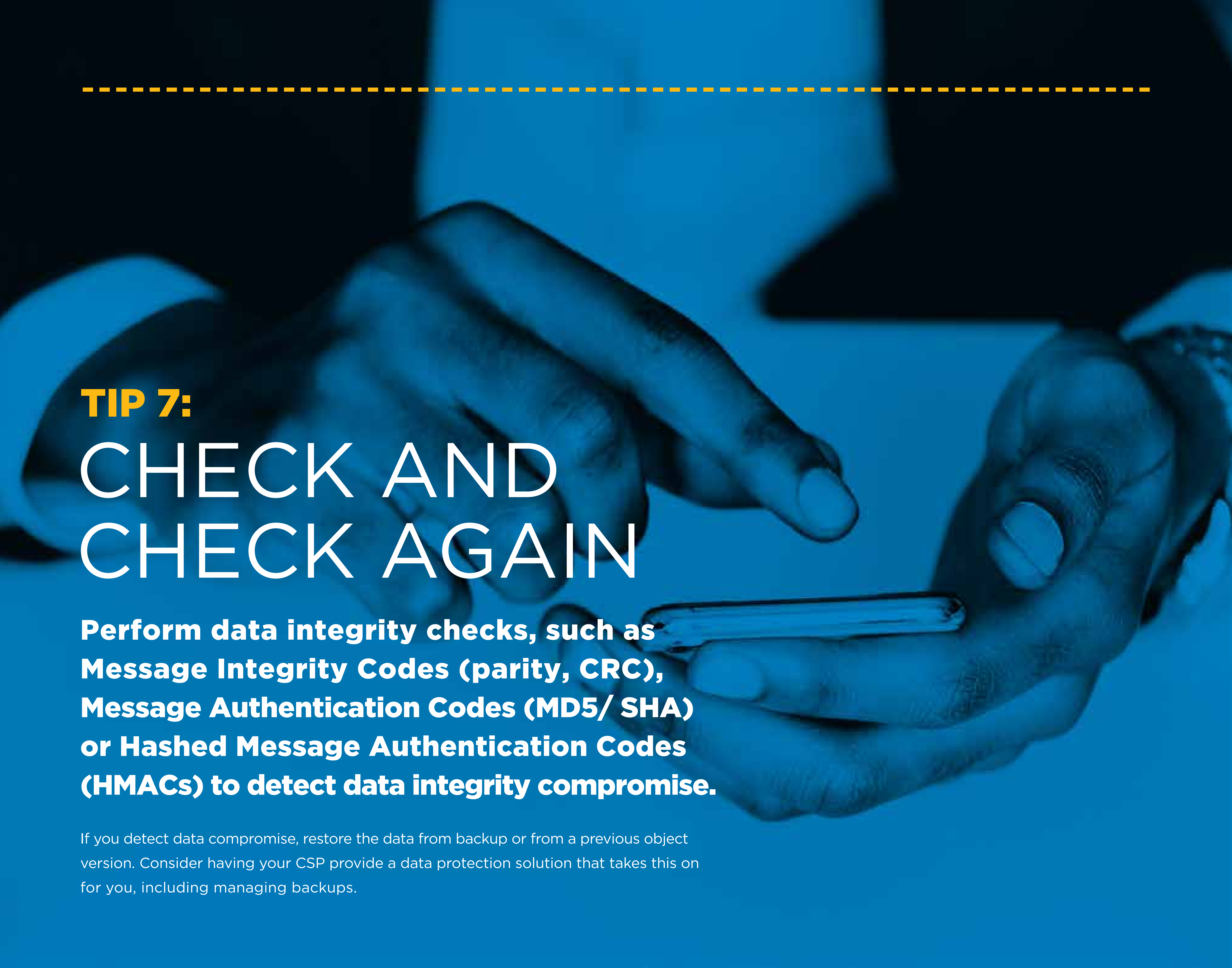
This can be done with initial system hardening when you create the images. Take advantage of technologies that enable you to update the images offline with the latest service and security updates.

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.

If you’re considering procuring cloud services from a CSP, opt for those certified to meet PCI DSS or HIPAA compliance requirements — even if your organization isn’t in an industry that requires compliance with those standards.

PCI- and HIPAA-compliant cloud environments employ infrastructure and processes that enable them to meet very stringent security requirements. That translates into a more secure cloud environment.

TIP 10:

SEEK COMPLIANCE

TIP 11:

REQUIRE CSP TRANSPARENCY

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.

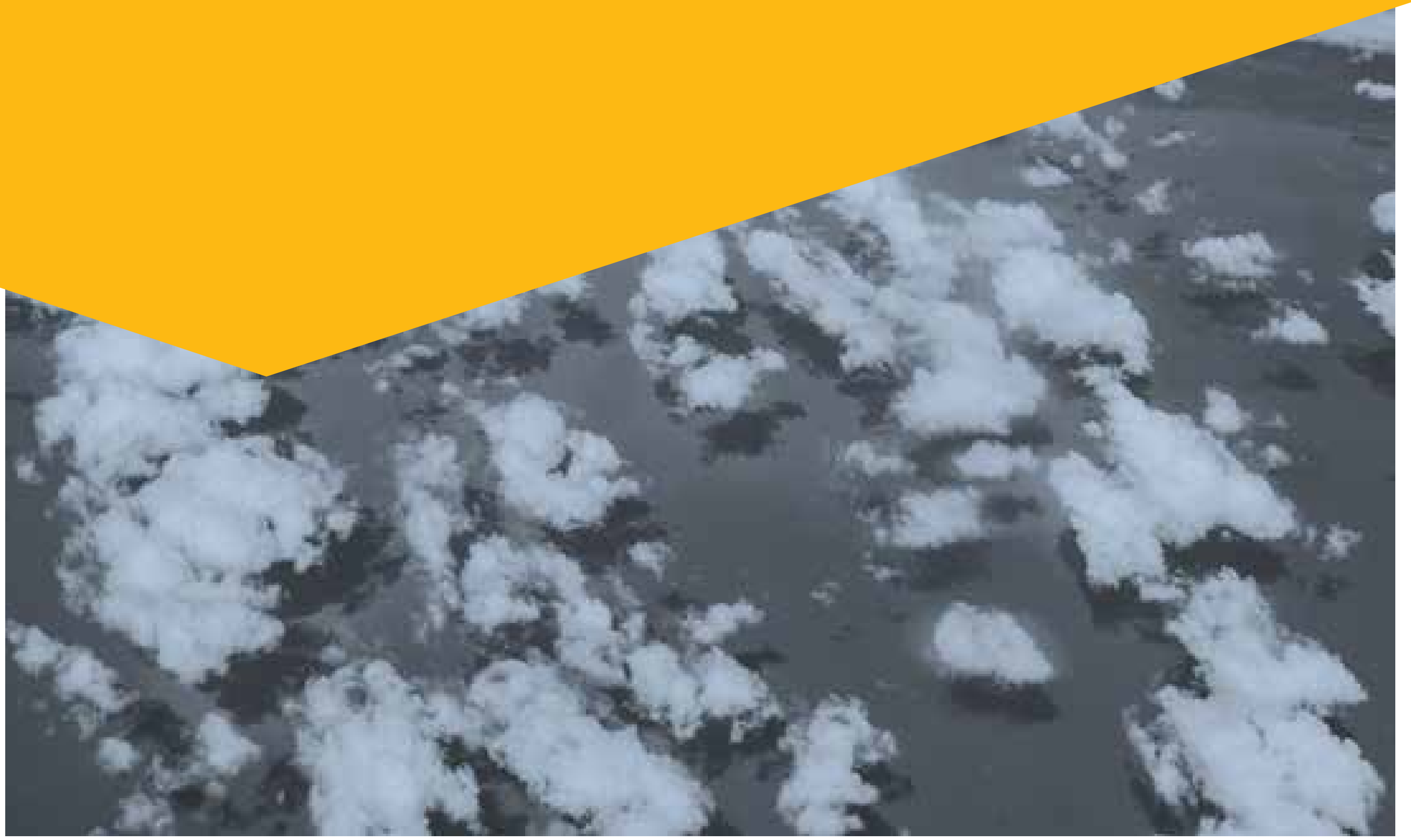
CSPs should be able to provide log files, reports and applications that allow you to view data traversing their virtual networks and events within the cloud in near real time.

Use your web proxy, firewall, or SIEM logs to discover what cloud services are being used that you don't know about. Then run an assessment of their risk profile.

The rapid growth of cloud-based consumer applications has increased the adoption of shadow IT — the use of IT systems, devices, software, applications, and services without IT department approval. You can also gather information about what programs are currently used and what they're used for through employee surveys.

TIP 12:

UNCOVER SHADOW IT



TIP 13:

SCAN FOR VULNERABILITIES

Use vulnerability scanning tools or a vulnerability management service to identify security holes across servers, firewalls, and more. Conduct both external and internal scans.

Most scanning tools can classify and categorize vulnerabilities to help prioritize the most serious issues. Some also facilitate the creation of reports about a network's security status once vulnerabilities have been addressed. This is important if an organization is required to show compliance with certain regulations.

TIP 14:

PROTECT ENDPOINTS

Monitor, detect and remediate threats across endpoints such as laptops, desktops and servers with an endpoint detection and response (EDR) or a managed endpoint detection and response (MDR) solution.

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 15:
PAD YOUR PLAN

Include data protection, backup and recovery as part of your cloud security plan.

A secure environment doesn't mean a cyber attacker can't find a way to at least slow down your operations or corrupt your data. The right data protection, backup and recovery tactics can help ensure that if your cloud security doesn't stop an attack, the data and applications you need most will still be accessible and usable.

THE REALITY OF CLOUD SECURITY

Accept that there is no such thing as a 100% secure cloud environment. When you assume your cloud environment is impenetrable, it's easy to become lax about security best practices, regular audits, employee security awareness training, and other elements.

What protects against threats and vulnerabilities today may not work against what they'll morph into next month. Working with a CSP or managed security company that stays on top of the latest threats is important. But it's equally essential for your IT staff to keep pace with what's happening on the security front as well. Follow a few blogs written by trusted security experts or cloud companies. Attend IT security webinars. Take advantage of information provided by vendors and technology partners. Most important, never let your guard down.

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**