MARK43

Making Data Security a Priority

How law enforcement agencies can ensure their technology vendors have critical security measures in place—a must in today's high risk environment

Larry Zorio, Chief Information Security Officer at Mark43

Cybersecurity is as important to public safety agencies as the physical lock on the door of a building. Public safety agencies operate in a high risk environment, with constant risk of cyberattacks and penetration threats. Security measures must be constantly evolving.

The public expects their law enforcement agencies to have the strongest cybersecurity defenses - but how can these agencies trust that their technology vendors take security seriously?

There are a number of security issues and concerns that should be top of mind for any public safety agency working with technology vendors. These agencies should be conducting security reviews of any potentially new or existing vendors or service providers on an annual basis. However, most agencies do not have the time or resources to audit the vendors' security controls themselves. So how can agencies know whether or not their vendors are meeting applicable security standards and keeping their data secure? First, agencies should always request a vendors' SOC 2 or SOC 3 Report.

An overview of SOC 2 compliance

SOC 2 (System and Organizational Controls) is a controls audit standard that focuses on security, and where appropriate can go deeper into additional confidentiality, integrity and availability controls. A successful SOC 2 audit can be seen as a verification that a company's security protocols are not only in place, but are being followed. While these audits and reports do follow basic criteria, they can be very different from one SOC 2 report to another.

A SOC 2 report should include the following components:

- Control Environment
- Communication & Information
- Risk Assessment
- Monitoring Activities
- Control Activities
- Logical & Physical Access Controls
- System Operations
- Change Management

While any vendor can say they are mature in these areas, it's best when agencies can verify this, and that takes time. A SOC 2 audit can help solve this problem, as a SOC 2 audit involves a vendor hiring a third party to come in and audit their security program. A SOC 2 audit can be a great tool for an agency as it provides an independent verification of a company's security controls.

> While any vendor can say they are mature in these areas, it's best when agencies can verify this, and that takes time. A SOC 2 audit can help solve this problem.

The two types of SOC 2 audits

There are two types of SOC 2 audits: SOC 2 Type I and SOC 2 Type II.

- **SOC 2 Type I** is a single point-in-time audit. An auditor will arrive on a given day and ask to see in-scope policies, procedures and controls. They will verify that these all exist and are being followed, but only at the time of the audit.

- **SOC 2 Type II** takes place over a period of time. Typically, either a six month or—ideally—a year-long audit period. A SOC 2 Type II means the auditor is actively engaged and is asking for examples throughout that period of time. An example of this could be reviewing change management requests throughout the entire year. The ability to review a vendor's controls throughout an entire year can be extremely valuable to an agency.

Please note, this document will focus on a SOC 2 Type II only. A company that only provides a SOC 2 Type I is most likely either a newer company or one that does not prioritize security diligence for their customers.

Security best practices to look for in your vendors

The criteria areas listed above are a great start, but it's also important to dive deeper into the SOC 2 report and look for best practices. Some of these will provide insight into the maturity of an organization. Examples of best practices include:

Risk management

The vendor should be managing both internal and external (e.g. supplier) risks on a regular basis. Internal risk management could be assessing risk to make decisions on development and controls activities. From an external perspective, their supplier's controls should be reviewed, similar to what an agency does with SOC 2 reports.

Change management

The vendor should have formal checks and balances when it comes to making changes within their environment. First and foremost, these changes should be documented with a formal approval process that is separate from the person making the change.

Access management

Access management can be a very broad category, but it’s best to focus on inspecting processes around adding, changing, and removing a user’s access. Additionally, confirm that privileged accounts (e.g. administrative accounts) have additional layers of controls attached to them.

Vulnerability management

Verify that there are controls around identifying and remediating vulnerabilities in all layers of the tech stack (e.g. Application code, servers.)

Information security

This too can be a very broad category, but at a minimum agencies should look for endpoint protections, virtual private networks (VPNs) and multi-factor authentication (MFA). An agency should look internally at their own basic controls and ensure that a potential vendor maintains at least the same standards.

Data protection

Vendors are often the stewards of an agency’s data. This data can be extremely sensitive, and include criminal records, financials, medical records, and more. Agencies should ensure their vendors are using encryption methods both in storage and in transit.

Incident response

Technology vendors should have a formal process to manage a cyber incident. When contracting with a vendor, a public safety agency must ensure that the vendor is taking the availability of the agency’s data and service seriously. Agencies should verify that the vendor has business continuity and disaster recovery plans in place, and that the SOC 2 auditor has tested controls around that plan.

Business continuity

When contracting with a vendor, a public safety agency must ensure that the vendor is taking the availability of the agency’s data and service seriously. Agencies should verify that the vendor has business continuity and disaster recovery plans in place, and that the SOC 2 auditor has tested controls around that plan.

There are three critical components to protecting networks, infrastructure, applications, products, and data, referred to as the Security CIA triad: Confidentiality, Integrity and Availability.

- **Confidentiality** — Agencies need to know that their data is protected from unauthorized access
- **Integrity** — Agencies have to be able to trust their data
- **Availability** — Agencies need to be able to access their data

> There's an old proverb that says, 'A threefold cord is hard to break.' Confidentiality, integrity, and availability work together to provide a functional and secure environment for mission-critical systems and data.

Limitations to a SOC 2 report

Although a SOC 2 report is a valuable tool to evaluate a vendor's security standards and protocols, a SOC 2 report contains sensitive information and should not be broadly shared. Agencies and vendors often need to exchange a non-disclosure agreement (NDA) in advance of sharing the report. A company's SOC 2 report is typically only shared with a potential partner once that NDA is in place, or an actual contract has been initiated. Both of these take time.

The value of a SOC 3 report

A SOC 3 report is a step beyond a SOC 2 report, and solves a confidentiality issue. A SOC 3 report is a document that verifies that a SOC 2 audit has been performed but it does not reveal any sensitive information (i.e. details on controls). A SOC 3 report is a public-facing document intended for a general audience. No NDA or contract is needed to view a SOC 3 report, or even any interaction between the vendor and a potential partner. Many companies post their SOC 3 report on their website for others to verify on their own.

A SOC 3 report is another tool to help perform due diligence on a vendor. It helps both vendors and agencies in two ways:

1. Agencies can very quickly go to a website and get a high-level idea of a vendor's maturity. It can be part of an early vetting process of an organization and a potential partner, before contracting even starts.

2. From the vendor's perspective, it gives potential partners assurances about their security without having to begin the lengthy process of an NDA or contract, which can slow things down.

Mark43's SOC 3 report is available here.

The public safety community is expected to provide the highest level of integrity in every aspect of their work. To ensure this, public safety agencies need their partners and vendors to maintain the highest standards of security as well. A good foundation is the SOC 2 and SOC 3 report. The independent verification provided by these tools are a critical step toward ensuring data security and cultivating public trust, and public safety agencies are strongly advised to choose partners that have met these requirements.

Larry Zorio

Larry Zorio, Chief Information Security Officer at Mark43, and his team are responsible for protecting the confidentiality, integrity, and availability of both enterprise and customer data, assets, networks, and products while meeting public safety agencies' unique security needs worldwide. Larry has more than 20 years of cybersecurity experience, helping organizations manage risk and chart a cyber-focused path in this ever-changing technology world.

About Mark43

Mark43 is the leading cloud-native public safety technology company. By delivering a modern, intuitive and mobile-first Records Management System, Computer-Aided Dispatch and Analytics platform, Mark43 empowers governments and their communities to improve the safety and quality of life for all. With more than 120 local, state and federal public safety agencies, Mark43 is transforming how first responders use technology to respond, engage and serve the community. Mark43 provides the tools, resources, expertise, and security foundation that public safety needs today, tomorrow, and beyond. For more information or to request a demo, visit www.mark43.com.

MARK43

mark43.com | info@mark43.com | 212.651.9154