# Data Protection Tools

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

*http://bit.ly/2BK5W7C*

Data protection is critical, but it can sometimes be less visible than other types of security controls. This is because, very often, data protection failures are contributory rather than directly responsible for security failures. In other words, the direct cause of a high-profile breach may be something not related directly to data protection, but data protection often causes the impact to be significantly greater or the scope of compromise to be much broader because those controls are not in place.

To illustrate this point, consider a breach such as Equifax. By now, most professionals know that the direct cause of the Equifax breach was related to patch management—specifically, failure to patch Apache Struts. However, it is also true that data protection might have played a contributory role in the resultant scope and impact of that event. For example, would the breach have been as impactful if the data were encrypted? Would the actions of the attackers have been noticed in time for the security team to take action if better exfiltration alerts had been in place? We will never know the answers to these questions, but we can surmise that, had data protection measures been in place, at least some of the scope or impact might have been mitigated.

It behooves practitioners, therefore, to understand and employ data protection measures as a part of the security and assurance tasks they undertake. It is, of course, optimal when the organization's practitioners can invest in tools that directly support data protection measures. However, practitioners do not always find themselves in "optimal" situations; that is, organizations can directly and immediately invest in data protection measures only some of the time. But immediate benefit can be gained when practitioners can adapt investments in data protection goals or tools that already exist in the ecosystem. For the savvy practitioner, this represents a potential quick-win—an area where one can move an assurance or security goal forward based on investments the organization has already made.

There are, literally, hundreds (if not thousands) of tools that can be purchased, adapted or applied to forwarding data protection. The tools discussed here are a starting point—some that are useful to practitioners across a broad swath of industries, areas where one or more tool investments are likely to already exist in the ecosystem, and those that are likely to be useful regardless of whether the practitioner is an audit, risk or security professional.

Ultimately, data protection should be thought through from the perspective of the goals the organization wants to accomplish. As practitioners do so, they may find opportunities such as those described here for adding value through the use of tools the organization is already using.

**Ed Moyle**
Is director of thought leadership and research at ISACA®. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers, and senior security analyst with Trintech. Moyle is coauthor of Cryptographic Libraries for Developers and a frequent contributor to the information security industry as an author, public speaker and analyst.

## 1 Data Discovery and Inventory cont.

Tools can play a beneficial role in discovering and inventorying what data are in an organization and mapping out where the data are stored, processed and transmitted.

It should be stated explicitly that the specifics of the data a given organization might wish to locate will vary based on the organization itself. While discovery and inventory of sensitive data are important regardless, the specifics of the data (and, therefore, the specific tools an organization might employ to find the data) are different based on the type of organizations are and the specific considerations they have.

This means that tools that support discovery and inventorying of data can directly assist practitioners in a few ways:

1. By helping them verify that other controls are performing as expected
2. By building out a "map" of where sensitive data live throughout the organization

Once this is complete, the tools can also be run periodically in *ad hoc* fashion to find and flag situations where data have been stored or transmitted to an unexpected location.

It should be noted that there are a few different categories of tools that can help in this regard:

- Commercial data discovery tools, which assist organizations in finding, collecting and consolidating data stores for business intelligence or advanced analytics purposes
- Data leak prevention (DLP) tools, which can be used in an ongoing way to find and flag data that should not be stored or transmitted through certain channels based on business rules, and can help to prevent data exfiltration
- For practitioners on a budget, special purpose tools can be useful, (e.g., tools such as ccsrch (PANs), hashfind/passhunt (locates passwords and related artifacts), and grep/egrep when used in combination with specially-crafted regular expressions

## 2 Data Encryption

There are also tools that help practitioners encrypt data where the data are stored or transmitted. It should be noted that there are absolutely any number of special-purpose encryption tools out there that can be directly employed or adapted to encrypt data at any level of the Open Systems Interconnection (OSI) stack—at the application layer, at the file system layer, for data in transit, etc. It is always the better option to systematically and holistically address encryption use, applying it in combination with something like a formalized threat modeling exercise to protect against known, analyzed and thought-through threat scenario. Such systematic analysis is the ideal case.

However, because the ideal case is not always the actual case in every organization, it is worth noting that practitioners have data encryption options even in the absence of that broader investment. First and foremost, most modern operating systems have file system encryption options built into them. In combination with data discovery and a reliable inventory, tools are often available natively on the operating system platform used within the enterprise. This includes tools such as BitLocker (Windows), eCryptfs or LUKS (Linux), and others on a platform-by-platform basis. Likewise, database and middleware software can sometimes support encryption natively within it.

Many cloud service provider (CSP) storage and computing implementations make encryption of data at rest and in transit directly available to the customer in such a way that minimal additional overhead (other than checking the box) is required. The mechanics of enabling this depend on the CSP and the platform the organization employs, but almost all serious providers offer this for storage, Infrastructure as a Service (IaaS), and in application programming interfaces (APIs) or other services for Platform as a Service (PaaS) implementations.

## 3 Exfiltration

There are many tools that the organization may already have in place that can be used to detect and alert on potential exfiltration activity. Any network monitoring device (e.g., firewall or intrusion detection systems [IDS]) can potentially be adapted to help provide value for an exfiltration scenario. Firewalls or HTTP forward proxies can be employed to look for suspicious outbound connections (e.g., entities that are on IP black lists). IDS devices can do this and also potentially be adapted to trigger on custom regular expressions that might correspond to sensitive internal information.

One important thing to note is that, for the purposes of exfiltration, many attackers will employ encrypted channels such as Transport Layer Security (TLS), Secure Shell (SSH) or even nonstandard encrypted communications techniques.

Therefore, while potentially a valuable addition, it cannot be assumed that an IDS (monitoring, as it does, plaintext traffic) will necessarily always be able to detect this activity. As such, keeping an eye out for suspicious connections is a useful step, whether or not the organization also employs an IDS to detect exfiltration.