

searchSecurity.in

Information systems audits must evolve to become information audits

Most organizations handling consumer data in segments such as financial services, telecom, utilities, and so on, have some kind of compliance framework ([ISO](#), [GLBA](#), [HIPAA](#), RBI or [SOX](#), for instance) against which periodic compliance audits are conducted. For example, an audit on the handling of credit card transaction data in a bank would include checking the perimeter security of the systems the data resides on; checking the encryption used to store the data; looking at each input and output point that touches the data; and, checking the levels of access each role/employee has to that data. An audit of such data would also include checking the process of backup, including following the backup tape in the armored van, all the way to the backup vault!

An audit such as the above recognizes that a leak from any part of the system renders the strength of the rest of the system useless. In such situations, the bank owns or tightly controls the entire value chain from the input of the data all the way to archive and storage. At no point is the data allowed to reside in the hands of a third party, without the third party being tied down with draconian penalty clauses for any leak that may take place for whatever reason. As the information is resident within a specified boundary, information audit is in reality a comprehensive information systems audit in this case.

Now take for example an audit done on a high volume transactional website that engages third-party shipment companies (to ship products bought on the website), third-party call center support personnel, and often uses third-party business intelligence companies to give insights into customer behavior and purchase patterns. In each of these cases, the data is shipped out or made available in real time to these entities. To strictly audit third parties in such cases is highly complex, if at all possible. Such third parties are usually scattered around the globe and often subcontract to work-at-home employees. Further, urgency of requirements along with costing constraints ensures that third parties are seldom compliant with industry standard security practices. Once the information has left your system, any checks done on the system are rendered pretty much useless, and this lack of “trackability” directly translates to a lack of accountability.

In this example, the information is not really contained within any perimeter, and any information audit should ideally cover all the systems the information touches through its lifecycle. This may include internal and external systems. Clearly, this is a very difficult task. In this case, an information systems audit is a poor way of performing the information audit. In reality, the thinning of the enterprise perimeter is forcing organizations to perform an information audit over and beyond the [traditional information systems audit](#).

Borderless information audit

Delve deeper

[The role of classification in data protection](#)

[Data classification as an insurance to protect information](#)

[Map your data classification policy to controls effectively: How-to](#)

[Four DLP implementation best practices from ISACA](#)

[6 information security risk assessment pitfalls to avoid](#)

Going beyond the semantics, this shift is a rather fundamental paradigm shift. Focusing the audit to the asset (information) over and beyond the cost base (systems) seems to be the correct approach, but is not very easy. An information audit covers the [complete lifecycle of information](#) — from creation to destruction.

According to Shashidhar C N, a director at ISACA, Bangalore, “Any data constituting sensitive personal information (SPI) needs to be encrypted at rest and in transit. If not, it’s as good as lost or misused. With increasing awareness of auditors in performing information audits rather than just system audits, and availability of technologies such as [information rights management \(IRM\)](#), companies no longer have an excuse for not protecting SPI data, or to claim that once the information has left their systems they are no longer able to control its use.”

There will be no real "boundary" of this information audit, since the information will span perimeters, countries, companies, applications, networks and devices. Given present day systems, this is a difficult activity to even know about, so the possibility of an information audit looks like a distant dream. Such a "borderless" information audit would involve processes and technologies that have the capability to track and control information usage across perimeters and to provide a central view of information usage through its lifecycle.

The good thing is that IRM systems are easily available, and can be deployed without the need for too much modification or customization. The not-so-good aspect is that IRM systems are restricted for the moment to unstructured information, and do not cover databases as yet.

About the author: Vishal Gupta holds a graduate degree from IIT Mumbai and is founder and CEO at Seclore. He is a specialist in fingerprinting technology founded Herald Logic in 2000 before starting Seclore. His other areas of expertise are information usage control, information rights management (IRM) and secure outsourcing.

You can also subscribe to our twitter feed at @SearchSecIN

19 Jan 2012

All Rights Reserved, [Copyright 2009 -2012](#), TechTarget | [Read our Privacy Statement](#)