COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Protecting Data From Inside and Outside Threats

By Karen Kroll

Organizations' responsibility to secure the data they collect, both from within their operations (say, intellectual property) as well as from customers (such as credit card data) continues to escalate.

In part that's due to consumers' growing interest in businesses' use of their personal information. More than half the respondents to a study done last year by Consumers Union, publisher of *Consumer Reports*, expressed concern about companies holding onto their data even after the companies no longer need it.

Moreover, the threats to which companies are vulnerable show no signs of dissipating. Almost one-third of companies responding to the 2012 Cyber-Security Watch Survey said the number of security events at their organizations had increased in the last year.

No surprise, then, that government officials are taking a stronger interest in companies' data protection policies and abilities. Case in point: the recently released publication, "Privacy on the Go" by Kamala Harris, attorney general of California. The "privacy practice recommendations" outlined in the document apply to mobile carriers, device manufacturers, and others in the mobile industry. One such recommendation directs application developers to limit their collection of personally identifiable information (PII) that isn't needed for their app's basic functionality.


Harris

Critics of Harris' move have cast it as a maneuver around proper rulemaking channels, but compliance officers "are saying that they don't have the luxury of deciding if it's legal or not," says Scott Vernick, a lawyer at the law firm Fox Rothschild who focuses on privacy and technology. Instead, they are trying to work with the recommendations as they formulate their data security approaches.


Vernick

Emerging Best Practices

While most compliance officers long have recognized the need to protect data, the processes and tools they use to do so continue to evolve and advance. Sophisticated companies, Vernick says, keep in mind several principles that have won support from regulatory authorities as they formulate their data security approaches. They are:

- Collecting only the data a company truly needs;
- Restricting access to that data only to the people who truly need it, for only the minimum amount of time necessary;
- Adhering to the data protection policies the company communicates to customers and clients.

With these principles in mind, Vernick continues, a first step in properly protecting data is an audit. Compliance officers need to know:

- What data their firms have;
- Why they have it;
- How it's being used;
- Who has access;

FEELING SAFE IN THE CLOUD

So what if your IT infrastructure is nothing more than rented cyber-space? The growing use of cloud service providers does have an effect on data security, says Danny Creedon, managing director with Kroll Advisory Solutions' cyber-investigations practice. While moving functions to the cloud can streamline an organization's operations, it also can complicate the data security picture.

As a starting point, responsibility for securing data always rests with the company, regardless of whether it stores that data in the cloud. "You can't outsource risk management," says Matthew Butkovic, technical portfolio manager at the CERT Program at Carnegie Mellon University.

Still, cloud storage can now be easily established by any employee, well outside the company's standard purchasing or contract management process, Butkovic says. That can mean the agreement isn't given proper scrutiny. Step 1, then: "Understand who in the organization has authority to charter these relationships."

The organization also needs to understand the limits of the cloud provider's responsibilities, especially concerning security. This isn't always easy to figure out. Some cloud vendors give customers (especially small ones) only limited visibility into their internal security processes and technologies, Butkovic adds.

To gain an understanding of a cloud provider's data protection policies, Creedon recommends asking for what's known as a SOC 1 (Service Organization Controls) report. "These detail to the letter what they've put in place regarding security," Creedon says.

A SOC 1 report evaluates the cloud providers' controls that are relevant to their client companies' internal control over financial reporting. The reports are prepared in accordance with the Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization. While the cloud providers pay for the reports, they are prepared by third-party auditors.

Compliance professionals also will want to be familiar with the IT audit and assurance standards developed by ISACA (formerly the Information Systems Audit and Control Association). ISACA audit standards often are used in both internal and external audits, Butkovic notes.

Liability for breaches and service disruptions "is becoming contentious," Butkovic adds. For example, some cloud providers want to limit their liability to 12 months of service costs. The upshot? Cloud users need to read the fine print.

—Karen Kroll

Reprinted from Compliance Week, March 2013

» Why they have access;
» For how long they have access.

Another key is obtaining a solid understanding of the enterprise architecture, says Chris Trautwein, chief information security officer with the International Information Systems Security Certification Consortium (ISC²). That is, where does the data reside, and what systems interact with it? The objective is to ensure you're protecting all possible points of entry to sensitive information.

Once an organization has a handle on the data it possesses, it needs to develop appropriate security policies and rigorously enforce them, Vernick says. Developing a policy that then is ignored is "like a plaintiff's lawyer's deposition outline," he warns. You don't want to commit a plan to writing if you're unable to follow through.

Also critical are "diligent data owners," says Danny Creedon, managing director with Kroll Advisory Solutions' cyber-investigations practice. That means, for instance, that the individual in charge of accounts payable should be responsible for regularly reviewing the AP files, checking who has access to them, and investigating any data access anomalies, such as an attempt to get into the files from outside the corporate network. "You need to make people accountable for verifying that the data is appropriately protected."


Creedon

> "You need to make people accountable for verifying that the data is appropriately protected."
>
> Danny Creedon, Managing Director, Kroll Advisory Solutions

A rigorous data classification scheme is also necessary, Creedon says. Categorize data based on its level of sensitivity; the less sensitive the data, the less protection it needs. (To a certain extent, the concept isn't much different than the risk assessments and subsequent internal controls that compliance officers employ for anti-bribery, fraud, or other risks.)

Larger organizations can use "good" and "bad" teams to test their IT security practices, Trautwein says. Under typical simulations, the bad guys try to identify and exploit vulnerabilities in the system, while the good guys try to thwart their efforts. Each needs some autonomy, but if they collaborate where appropriate, ultimately the company can use their findings to improve the effectiveness of existing controls, as well as implement additional controls to address any gaps.

Technical Tools

Current technology available to protect corporate data puts more emphasis on detective systems and controls than preventive ones, Trautwein says. Ideally, those new detection controls will complement the prevention controls you should already have in place, and help you understand how well the prevention systems are or are not working.

For example, if an employee should have access to the corporate network only during standard daytime office hours, the detective system should pick up any attempts to access the system after hours, and whether the attempt was successful. Simply knowing when someone is improperly nosing around corporate data is often invaluable, since, frankly, hackers will always be devising new ways to break through the prevention controls. The trick is in knowing when they do.

Several factors are driving the increased interest in detective tools. One is the amount of time necessary to identify a breach. In a large financial services organization, this currently runs about 32 months, according to a 2012 study from the Carnegie Mellon Software Engineering Institute. "You want to narrow the window," Trautwein says.

Ideally the detection systems would pick up malicious activity, such as an unauthorized attempt to access the system, before it escalates into a breach. If a breach does occur, earlier detection can limit the scope of damage.

That's crucial, given that "when a genie is out of the bottle, it's out of the bottle," says Matthew Butkovic, technical portfolio manager at the CERT Program, an IT security research unit at Carnegie Mellon University. In other words, it's very difficult to somehow "re-privatize" information that's been made public.


Butkovic

And the need to secure data is likely only to intensify, Butkovic says, given that most organization's databases are increasing in size, scope, and complexity. As a result, the processes and technology put in place to safeguard data must also be able to evolve and grow as the volume of data does. ■

ABOUT THIS SERIES

Compliance Week's exclusive new series "The Lifecycle of Information Governance" is sponsored by HP Autonomy. This six-part series examines all the elements of handling information properly—from creation to storage to destruction—and how compliance departments should address each element.

This month we focus on all things data, with features on how to protect your company's data from both inside and outside threats, and how to properly classify data to guard against risk (Page 48).

Coming in parts 5 and 6 in May, we'll cover monitoring of data use and destroying data when the time comes.