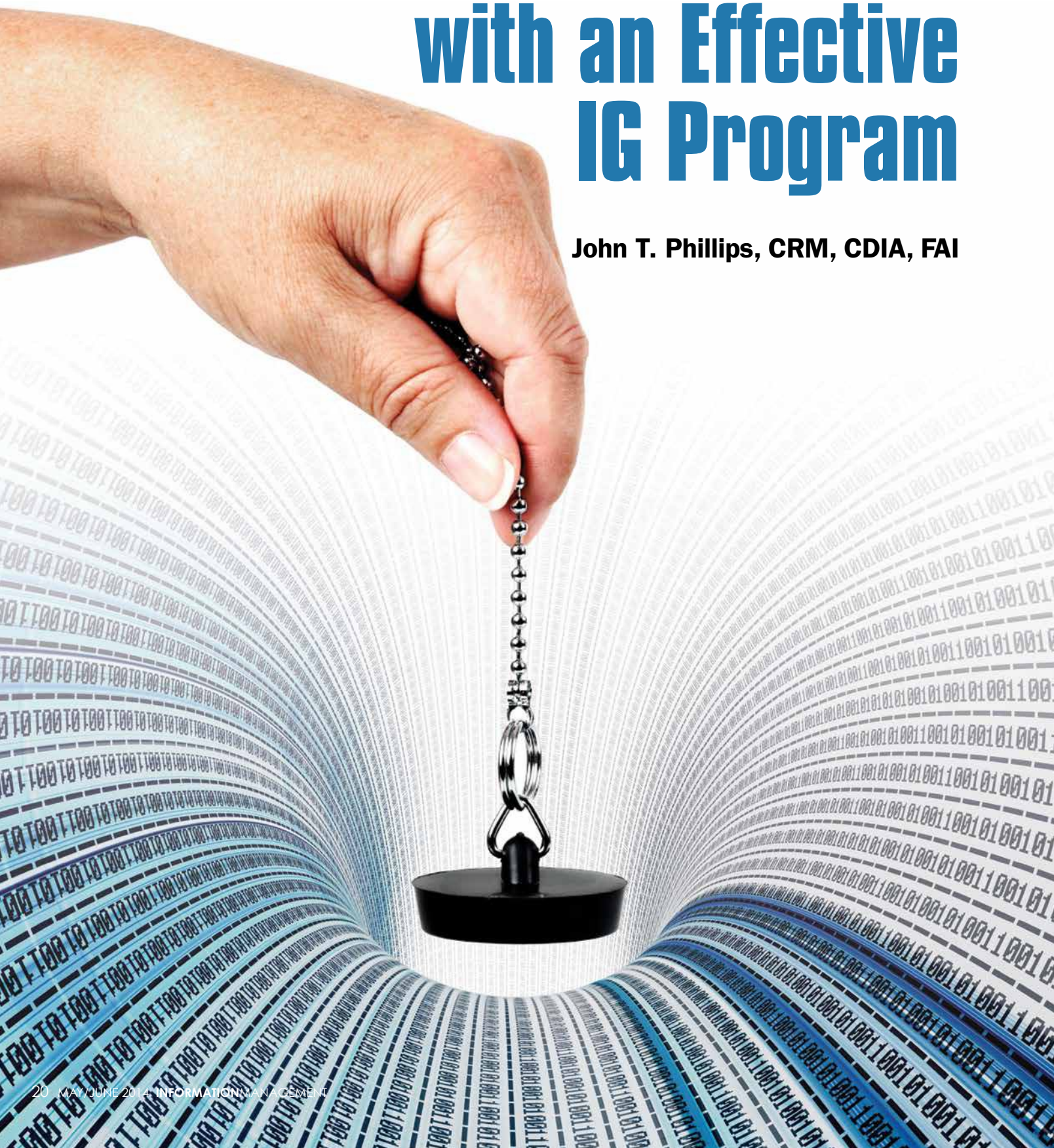
Plug Internal Data Leaks with an Effective IG Program

John T. Phillips, CRM, CDIA, FAI



Increasingly, employees are selling the "crown jewels" of their organization's proprietary information for a pittance. Organizations are scrambling for ways to reduce, if not eliminate, these internal threats. An effective information governance program can help.

Today's information security dangers while "surfing the Internet," downloading applications to smartphones, and opening e-mail are well-known. Organizations expect network hackers, data thieves, scam artists, and phishers to act from external sources. But, the unsettling truth is that data breaches often originate from individuals who operate from within.

New Technologies Not Always the Solution

Because organizations have used IT-based systems for more than 30 years, it would seem that common data protection mechanisms would protect them from data breaches. Although technical solutions like increasing network firewall capability or implementing better user access control systems might have addressed security risks in the past, today's environment is more challenging. Trends like employees using social media and their own devices for business produce evolving risks, making it more and more difficult for IT to address them.

Buying sophisticated new technologies is not necessarily the answer, either. Buying a new solution to control every new technology that enters the market or respond to information trends will break almost any IT department's budget. And many, if not most, security technology solutions today focus on external threats rather than risks that are embedded in every organization that has employees.

Unfortunately, such measures as data archiving, log-on procedures, disaster planning, and data encryption are not sufficient safeguards if employees fail to rigorously and properly practice them. Indeed, in *Information Week's* "2013 Strategic Security Survey" report published last June, 42% of respondents said "enforcing security policies" was their biggest information security challenge. (See Figure 1.)

One respondent said, "Shops doing security right have moved away from gimmicks to analyzing the core of every other business discipline: people." Further, 54% of respondents said that end-user security awareness training was their "most valuable security practice." (See Figure 2.)

Insider Threats Are Difficult Challenges

It was once possible for IT to focus most of its data security activities on the detection of inappropriate intrusions into computer networks based on external Internet protocol (IP) addresses or inappropriate data traffic on computer networks at certain times of the day. Today's mobile workforce and 24x7 workdays have made those parameters of network security less relevant.

IT departments dealing with huge volumes of data traffic must differentiate risks that occur from outside an organization from those that occur from within because internal breaches can pose much larger threats. Two recent high-profile cases illustrate this enormous change in attention.

WikiLeaks

Australian journalist Julian Assange and the WikiLeaks website he co-founded cannot publish secret information without it coming illegally from sources within other organizations. In the largest release of classified government information in the history of the United States, WikiLeaks was aided by U.S. Army soldier Pfc. Bradley Manning. Manning, who downloaded nearly 500,000 war documents to a compact disc, later copied the files to his laptop, and then transferred them to an SD card for a camera to transport them, provides a prime example of the risks of insider data theft and mobile technologies. In addition, the fact that an organization like WikiLeaks exists and has some public support for posting confidential insider information should give IT system administrators pause.

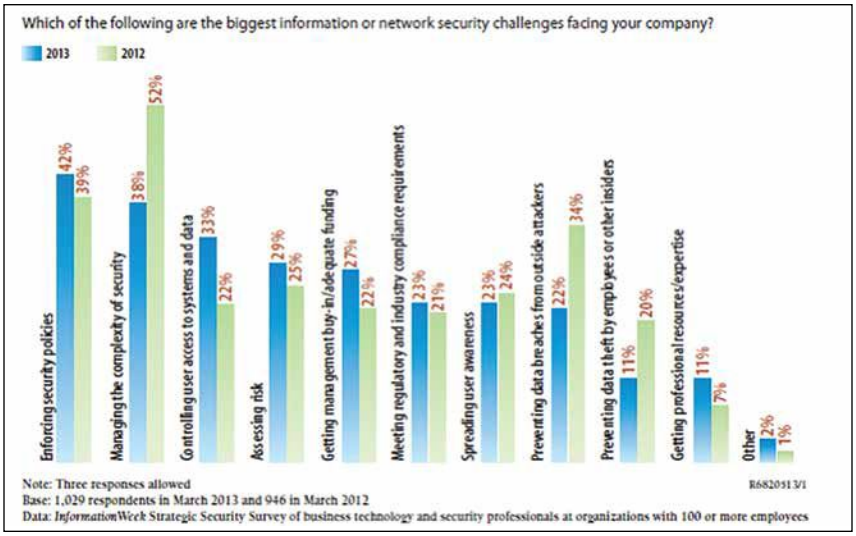


Figure 1: Biggest IT Security Challenges

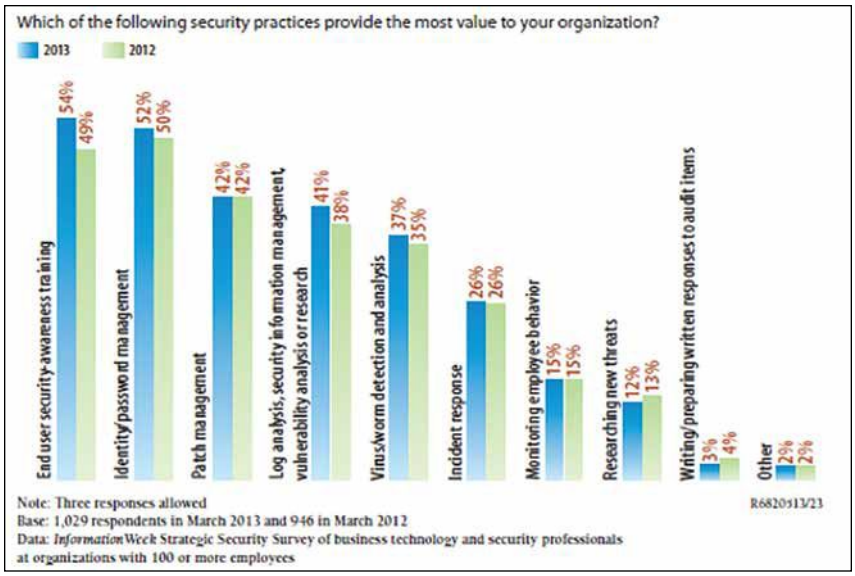


Figure 2: Most Valuable Security Practices

NSA Files Theft

More recently, U.S. National Security Agency (NSA) contractor Edward Snowden released approximately 1.7 million internal intelligence files, starting an enormous debate about the role of the NSA and other organizations in collecting information on private citizens and foreign leaders. This case makes it obvious that internal data breaches can have far-reaching organizational and social impacts.

Responses to insider threats can be difficult to incorporate into IT department strategic plans. How does an organization develop metrics for the frequency with which employees store company data on personal devices, for example?

Information Volume Overwhelms Tools

The tools that do focus on internal threats have only limited success. These tools often use technology that monitors external access threats to internal data and are designed also to monitor internal information being transmitted to external recipients by e-mail or by accessing external websites.

By monitoring large data transmissions, IP addresses for internal/external communications, and user system security parameters, IT system administrators can see if unusual data transmissions are occurring. Unfortunately, this approach is often overwhelmed by the sheer volume of information to analyze and results in reports without sufficient specificity to initiate meaningful security interventions before a compromise begins.

Focusing on Users, Content Can Help

So, how can IT departments increase the effectiveness of their internal security measures and internal system monitoring?

One method is to increase the specificity of the risk assessment by associating risks with data classification and users' access attributes. For instance, because it is possible to know that large data transmissions are atypical for some users, IT professionals can apply additional security measures to their user accounts.

They should apply these same measures to the user accounts of resigning or soon-to-be-terminated employees, who may be disgruntled and engage in data theft or sabotage before, during, or after their departure. With appropriate human resource procedures in place for data security, these breaches could be reduced in volume and severity.

Security monitoring is most effective, though, when the security measures can focus on the actual content of the data stream, discerning the increased risk when very sensitive information is crossing a network boundary, as opposed to monitoring large volumes of undifferentiated data. If, for instance, an e-mail contains certain text or metadata known to be business sensitive, additional attention must be focused on that data to effectively monitor the increased risk.

IG Program Is Best Solution

The best solution, though, is a comprehensive information governance (IG) program, which ensures that increased security measures and user training become part of an organization's daily operations. It is not difficult to develop an IG plan with strong information security awareness components that can be implemented by all employees and will enable them to intervene early in potential data breaches and minimize their consequences. Typical IG program components that can impact data security are listed below.

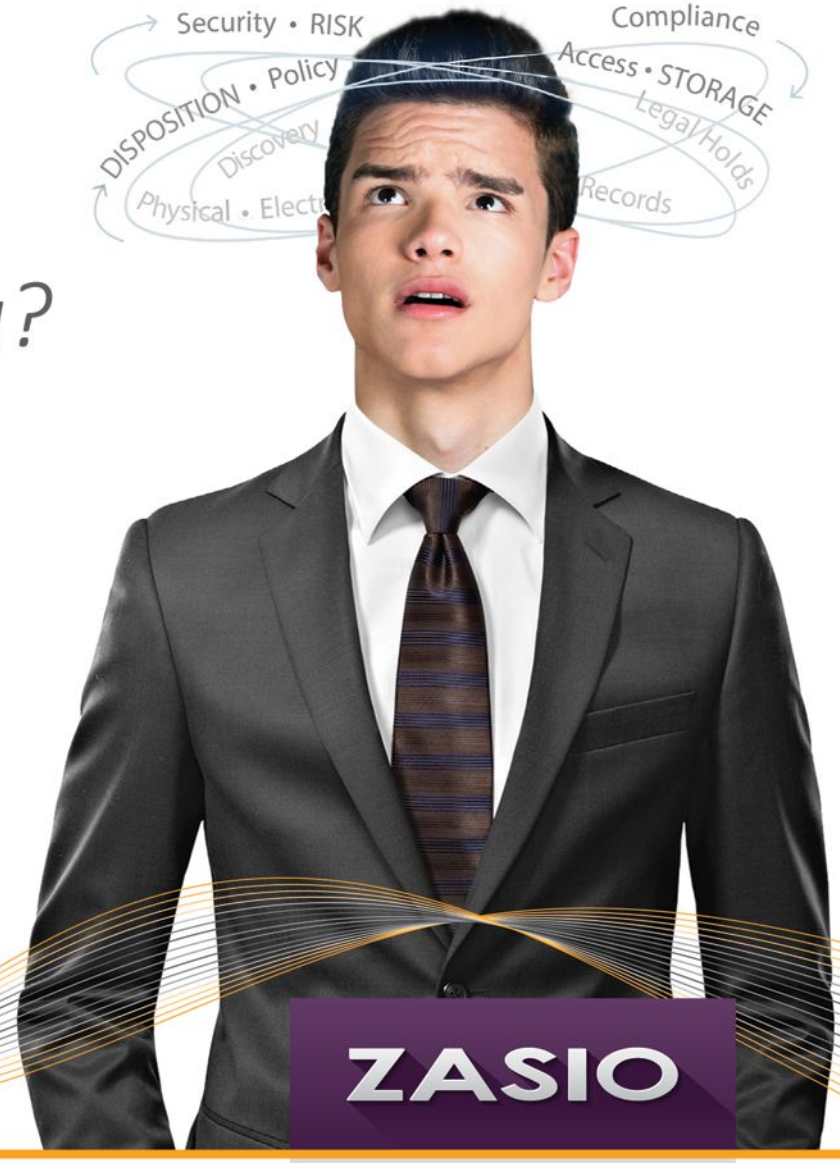
Data Management Policies and Procedures

Data management policies and procedures that address the enterprise-wide use of information represent the first step in embedding secure actions into systems and in helping ensure that employees are handling information securely. They are the umbrella that keeps data breach attacks from raining on an organization.

No single employee or department alone can intervene in every possible breach event. By cooperatively designing organizational IG standard operating procedures to address all types of information, it is possible to encompass most, if not all, attacks that could occur.

Don't be one of the many organizations that only partially implements its data management policies and

Information Governance have your head spinning?



ZASIO

RECORDS & DOCUMENT MANAGEMENT EXPERTS

Wrapping your head around all the issues surrounding information governance can be overwhelming.

The experts at Zasio provide the assurance you need. Zasio can help prioritize your objectives, develop your strategy, and implement the tools unique to your organization.

Call the experts at Zasio to discuss your Information Governance questions and challenges today.

800 513 1000 | www.zasio.com

Connect with us:

www.facebook.com/ZasioEnterprises

www.linkedin.com/company/zasio-enterprises-inc.

procedures, though; this increases litigation risk, not only because of the gap it leaves in the IG program, but because it implies to a court that the organization is not properly concerned with conducting business ethically and effectively.

IT System Inventories, Data Maps

Without knowing the informational content of technology systems, it is impossible to appropriately apply security procedures and retention rules. The locations of data, data types, and applications used for data creation and management must be clearly defined and documented for IG policies and data security measures to be implementable. An organization cannot manage and secure data it does not know exists.

Information Classification, Retention Rules

The data's value and risk must be classified before proper security measures can be applied. Business sensitivity, regulatory compliance requirements, legal hold obligations, privacy mandates, and other retention rules demand that data and IT systems be assigned content descriptors and metadata so appropriate procedures can be applied.

Organizational file plans, retention schedules, IT systems inventories, and application metadata can serve to create initial data security taxonomies to describe and classify information. In many cases, due to the huge volume of data that an IG program must encompass, automated tools that employ sophisticated search algorithms can enhance the specificity of classification processes across large data repositories and reduce the time needed to identify and respond to data breaches.

Enabling Technologies

In some cases, additional technology tools can be used to direct the application of security procedures to appropriate data and systems. Software already in use to detect viruses, malware, and other intrusive threats can often be applied internally to e-mail systems, database servers, file shares, and applications. In addition, more sophisticated search software can categorize data and system content for increased scrutiny once the information in those systems has been classified or the data can be accessed directly.

Many organizations are using enabling technologies to reduce human involvement in information processing. When content management systems were implemented many years ago, it was soon discovered that end users were not properly classifying content because of time constraints, system limitations, and confusing terminology.

Many applications now have content search, retrieval, and classification capabilities that allow at least an initial assessment of the value and appropriate rules to be associated with information types. These can save time, create data management metrics, and improve auditing of processes for classifying information and applying targeted data security measures. In addition, technology-based solutions can often identify data breaches that may not be evident to human eyes.

Training

Because systems are created for people and operated by people, employee training is extremely important for all information management system implementations.

Even "automated" technology solutions must be developed by people after targeting the business requirements, configured by people to be focused on their specific work process needs, and then operated by those individuals to accomplish their objectives. Training is a cornerstone of any IG program because humans are still involved in some way with all data creation, storage, and preservation or disposal.

Because systems are created for people and operated by people, employee training is extremely important for all information management system implementations.

The means and mechanisms of employee training across an enterprise might include direct-to-employee e-mail announcements, company-wide web seminars, social media site postings, and online testing programs with auditable accountability. Without a firm understanding of the importance of data security policies and the consequences of data breaches, many employees may not be aware they are contributing to increased risks.

IT Must Leverage IG

Data breaches will continue to plague organizations that do not have comprehensive IG programs with accompanying integration of data security policies, procedures, and consequences for non-compliance. Considering that IG programs can reach across organizations to impact and train all employees, IT departments must take advantage of these enterprise-wide programs. **END**

John T. Phillips, CRM, CDIA, FAI, can be contacted at john@infotechdecisions.com. *See his bio on page 47.*