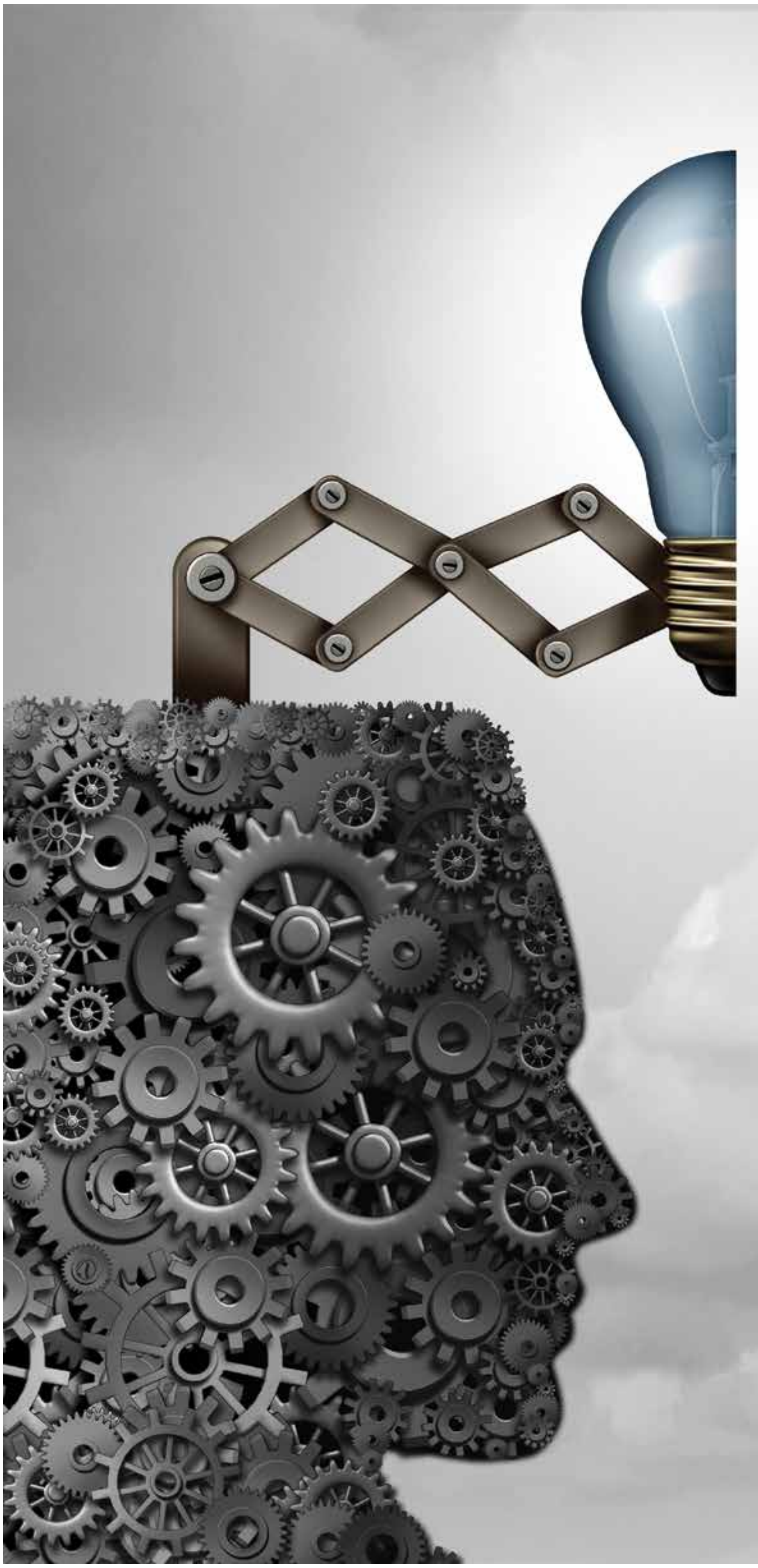
Teaming Information Governance and Security for the Best Defense

This article outlines a defensible strategy for securing assets based on information governance (IG) principles, and it suggests how IG and information security professionals can work together for a more secure and productive enterprise.

Galina Datskovsky, Ph.D., CRM, FAI



The number of ways bad actors are accessing corporate data and impeding organizations from serving their customers is on the rise. Information protection is paramount for every organization's ability to continue operating despite the daunting situations caused by cyber attacks and other out-of-course events, including natural disasters.

The Cyber Landscape

According to "Beazley Breach Insights – January 2017," the number of ransomware attacks the provider of data breach response insurance handled quadrupled in 2016, and it is expected to double again this year. Beazley also found that enterprises are most at risk when an IT system freeze is in place [to prevent system changes during an IT project], at the end of financial quarters, and during hectic shopping periods. Indeed, there are multiple news reports daily about another cyber attack, another data breach, and yet another leak of sensitive information.

Very often organizations take careful pains to protect their perimeters, but perimeters are now porous; information travels outside of them on laptops and personal devices and through communication methodologies like e-mail. Further, when a perimeter is breached, data repositories usually are not as carefully protected as they

should be. For instance, in many cases password protection and login information is through application access only; however, anyone with administrative access to a server can see the data quite clearly on the back end.

This is a great example of where information governance (IG) and information security (IS) professionals working together can help. IG can identify and rank systems based on their value and sensitivity, and they can identify information stores and the most valuable assets. Then, IS can better secure those systems and repositories, as well as the data itself, whether the data is at rest, in transit, or being accessed by mobile devices.

IG and IS: Perfect Together

To achieve true information protection, IG and IS professionals need to work in lock-step to ensure not only that the traditional perimeter is protected, but that multiple levels of security are implemented, down to the level of the data. By partnering, they can have a huge impact on their organization's security stance, ensuring that:

1. Business records are archived in an appropriate, secure repository (e.g., not in an e-mail account or left on mobile devices)
2. Accurate data replication has occurred so it is available to be used quickly in case of distributed denial of service attacks or ransomware infiltrations
3. Vital records are available in case critical procedures for recovery are necessary
4. Policies are applied based on regulatory, legal, and business requirements so records can be defensibly disposed of when their value has ceased

IS Needs IG

The focus of two large cybersecurity conferences this year illustrates that IS professionals need the influence of IG: the Gartner Cyber Security Summit, with more than 4,000 attendees and a great number of exhibitors, and the RSA Conference, probably one of the largest cybersecurity events in the world, with 45,000 attendees this year.

Despite a large number of presentations, only very few focused on the specific characteristics of data and how it could be protected if compromised. Many of the vendors focused instead on such things as protecting the perimeter of the organization, catching or preventing intrusions, and building better firewalls. These conferences made it clear that IS professionals have not spent as much time thinking about the protection of individual data assets as their IG colleagues have.

At both events, everyone readily acknowledged that it is essential to have the most up-to-date tools to protect organizations from a breach and that some of the most devastating attacks occur because of the lack of staff training. Attendees also concurred that the lack of data protection once the intruder gets in is a huge fail. Following are two examples of breaches that are quite telling.

Example One – Social Engineering

An assistant to the chief financial officer (CFO) receives an e-mail offering a coupon to her favorite shop. She opens the offer and perhaps even gets the promised $50 discount. However, her desktop is now infected with malware and the bad guys are in.

For a number of weeks, the hackers patiently monitor her e-mail, her calendar, and other system information. Eventually, they learn the chief executive officer (CEO) and CFO will be away on a particular Friday – the CEO on an international trip and the CFO on a retreat to a remote site – both without easy access to Wi-Fi or to landline phones.

While the CEO and CFO are gone, the crooks send an e-mail to the deputy CFO in which they claim to be the CEO and ask that $10 million be wired immediately to a certain site to prevent the organization from losing an important client. Not able to raise either the CEO or CFO to confirm the situation, the deputy CFO wires the money, which is then irreversibly lost.

The key points here are:

1. Staff was not sufficiently trained. Employees must be able to distinguish between genuine and fictitious inquiries. They need to see several examples of false messages and be trained to recognize any request for sensitive information.
2. Data was totally exposed when the perimeter was breached. An IG professional can help to add layers of data-specific security.
3. Better IG should have helped.

Read More About It

Charbonneau, Stephane. "Data Classification: Creating a Culture of Cyber Security." *Cyber Security Trend*, April 11, 2016. Available at *www.cybersecuritytrend.com/topics/cyber-security/articles/420021-data-classification-creating-culture-cyber-security.htm.*

Friedman, Ted and Tom Scholtz. "Align Information Security Governance With Your Broader Information Governance Initiatives." Gartner, 2016.

Gulzar, Remi and John MacDorman. "Enterprise Digital Governance: Resetting Governance for the Digital Age." Gartner, 2016.

Example Two – Wi-Fi Connections Compromised

Attackers manage to plant a trojan horse inside a large corporate network. In this case, they sit in a café that is frequented by the target's employees every morning. The crooks set up a hub that offers Wi-Fi service, hoping to entice the employees to connect their phones, smart watches, and other devices. The crooks' signal is disguised as one the customers are already familiar with and may already have in their devices' memories, and so many of them connect to it.

When the employees return to the office, they connect to the office network, which permits the attackers to penetrate unprotected and semi-protected data repositories in search of the types of data they can use to hold the organization hostage.

A key takeaway from this example is that when IG and IS work in separate silos, bad things can happen. Other key points:

1. Again, employees were not trained adequately to realize the dangers of connecting to open networks in public spots. They must know to connect only to Wi-Fi connections they can trust. They also should be instructed to delete their Wi-Fi histories so that information is not revealed to intruders.
2. Beyond that, more integrated IG is needed to more thoroughly protect sensitive repositories and therefore minimize the damage if intruders penetrate the systems.

Both examples point to the importance of protecting sensitive information and, significantly, the importance of assessing what the intruders are targeting. In a cyber attack, much of the breached information is derived from e-mail accounts, which often include sensitive messages that did not need to be retained, and from data on mobile devices that could have been removed as well.

Had IG – whose expertise includes analyzing data, implementing appropriate disposition, identifying the data to scrub, and identifying the vital records – been working with IS – whose expertise is applying security and disposition criteria to all data – the damage could have been minimized.

Steps to Take Together

IG and IS professionals must take steps to create a more secure data environment for their organizations.

Step 1

IG professionals should identify the following:

- Data repositories, machine or human generated, that contain particularly sensitive data, such as personally identifiable information, personal health information, or intellectual property
- The appropriate levels of sensitivity for the organization's information so, for example, a secret formula for a revolutionary drug is highly prowwtected while the marketing materials are given less security
- Opportunities for data anonymization and scrubbing for protection. For example, IG can help determine if sensitive information can be removed from a repository that is accessed by a wide range of users and connected to many systems.
- Repositories that are vital to business continuity and therefore need serious protection

Step 2

IS should augment the cyber-protection plan to work with the identified repositories to implement levels of protection that will make it very difficult for any intruders to access sensitive information. Accordingly, such protections will also make the recovery of a hot site much more efficient because all vital data would be readily available.

Step 3

IG and IS should work together to rid the organization of unnecessary information, including:

- Transitory, and yet potentially damaging, e-mail messages
- Transitory mobile communications, such as text and chat left on devices

Step 4

IG and IS should work together to ensure that mobile communication records, which need to be retained, are moved to a secure repository.

IG and IS as a Service

As was emphasized at one conference earlier this year, IS (like IG) has a difficult time getting the budget it needs because no one wants to fund risk. The challenge for IG and IS therefore is to reinvent themselves into a service that can help move the business forward. Following are some services they could offer:

- Scrubbing data of personal information and making it available to parts of the business that could use it but otherwise would not have had access to it
- Providing on-demand and value-based security
- Applying new security and IG processes to make them more customer friendly

As an example of the last service, consider a private wealth management function at a bank I work with. When a customer wants to make a major transfer, such as a charitable gift or endowment, it requires two-factor authentication. That is, at this bank, the customer must sign a transfer letter *and* authorize the transaction over the phone.

Because reaching customers on the phone is often a challenge, this process could be improved by using text messaging as the second factor. IG and IS could work together to enforce the appropriate disposition requirements for the texts on the phone and a more permanent retention at the bank. This change would likely be a win/win.

Making the Connection

Connecting the user experience and data to the security function makes both functions more accessible to end users. Offerings like this are more feasible when IG and IS work hand in glove to offer business opportunity. Finding entry points like this to provide a service to the business will provide quick success and true benefit to the organization.

About the Author: Galina Datskovsky, Ph.D., CRM, FAI, is CEO of Vaporstream Inc. The former senior vice president of information governance at Autonomy, an HP Company, senior vice president of architecture at CA Technologies, and founder and CEO of MDY Group International, is recognized globally as an expert in information governance and associated technologies. Datskovsky, who earned her doctoral degree in computer science from Columbia University, is a Certified Records Manager, a Fellow of ARMA International, and a frequent author and speaker. She can be contacted at *galina.datskovsky@vaporstream.com.*