Data Governance Strategies for the Digital Age

The digital age has forced many companies to alter—and sometimes completely revamp—data governance processes. Learn information management strategies that will help you deal with storage needs unique to the big data era.
New Threats, GRC Needs Upend Digital Age Data Governance

**Through the course** of everyday business activities alone, companies in the digital age generate, store and maintain a sometimes overwhelming amount of “big data.” The digitization trend has forced companies to alter—and sometimes completely revamp—information governance strategies and processes to adapt.

Big data governance obstacles don’t end there, either: A constant threat of data breaches complicates security processes, while regulatory compliance rules require innovative methods to track and analyze information to keep your company on the right side of the law. And, of course, the digital age provides businesses with access to unprecedented amounts of user data, raising ethical questions for corporations that tap into users’ private information for monetary gain.

All is not lost, however. With the right big data governance strategy, companies can make sure their information stays secure and regulatory compliant, while still taking advantage of the digital assets at their disposal. In this handbook, we’ll discuss the latest strategies to help organizations adapt to the increased storage needs, data-specific compliance mandates and security vulnerabilities unique to the digital age.

As information increasingly becomes an organization’s biggest asset, companies must continue to keep a close eye on governance processes to make sure they’re ready for the challenges presented by big data. We hope you find this information useful to help your business implement the latest data governance strategies and thrive in the digital age.

**Ben Cole**
Editor
SearchCompliance
The New Big Data Rules: Five Steps to Digital Information Governance

As data volumes increase exponentially, the speed at which they are created is also accelerating. The amount of data in the digital universe is astounding, with “geobytes” and “brontobytes” replacing terabytes as common data storage measurements. At the same time, governments continue to develop complex data management compliance rules.

The SEC’s new Regulation SCI was more than 700 pages. Industrial consortia also continue to write mandatory new rules or update long-existing ones like PCI-DSS. This combination of unprecedented storage needs and expanded compliance regulations makes it very difficult for organizations to get a handle on big data governance, but here are five strategies to help get you started.

Set Objectives
First, organizations must define information governance and its objectives differently. Information governance means nothing to corporate leadership unless it contributes to creating new wealth. After all, that is why companies exist. To succeed, information governance builds and enforces rules for digital information in order to create wealth. That new wealth is created by targeting two enormous baskets of hidden expenditures: the costs of finding data in everyday business and the costs of validating that data as factually accurate.

All of the rules, whether found in official regulations, consortia rulebooks or commercial agreements, exist to achieve one objective: creating data that can be relied upon as the truth.

When you connect the dots and show how information governance reduces costs, creates greater net revenues and achieves compliance, executive-level support is more easily achieved.
BAKE GOVERNANCE IN FROM THE START
Second, information governance must be included in the front end of any design process within the business. Ensuring privacy by design has become a popular best practice, but that only embraces one data classification: personally identifiable information. The same principles should apply to all business processes, whether renovating existing governance strategies or designing something entirely new.

In the 21st century, every process generates new data that must be governed. Establishing good governance rules in the very beginning creates enormous savings in later cycles because no one has to ask, “What do we do with all of this new data?”

Another, perhaps more meaningful, benefit when moving information into the front end of design is that intense focus is given to how new data will be used toward creating new wealth. Much of the new volumes of data are generated as very granular, observational data that doesn’t require governance, including keystroke monitoring, voice call recordings, application transactions and execution log data. But when we ask how that data improves corporate performance, there can be entirely different design outcomes.

MEASURE PERFORMANCE
Third, create the metrics that measure governance performance. Governance requires more than merely having policies and procedures in place and expecting associates and contractors to do the right thing. Enforcement of the rules must be included. That means being able to measure performance and quickly calculate when data is not conforming to the rules.

The metrics must focus on how both machines and human assets perform, especially because compliance risk is very likely to occur within the design of devices and the software applications that run on them. A nonreporting...
node on a complex system is often a first indicator of a much larger compliance problem, but if the metrics are not being measured, there is little chance to intervene early and limit potential adverse outcomes.

**ENFORCE YOUR RULES**

Fourth, invest in the resources that can, indeed, enforce your information governance rules. In the last two years, numerous major public hacks and system compromises have uncovered that prevent adverse outcomes adverse outcomes. The problem was no one was assigned the responsibility to review and respond quickly. Here is where connecting to the wealth creation objective becomes so important. Information security teams recognized long ago that the hardest part of their work is to investigate and discover the root cause of an adverse event. When that effort can be avoided, enormous cost savings are possible. But the solution has to include having someone ready to review, prioritize and investigate the metrics before the adverse event occurs.

Enforcing information governance rules does not require assigning human resources to endless, tedious reviews of log data. Applications and services can analyze the related log data for information security purposes. The competitive secret is to leverage those applications and services already in place at most companies to serve a larger agenda that includes information governance rules. Indeed, the Venn diagram overlap between governance and information security is becoming more and more substantial. This is because effective data security achieves much of what information governance is required to deliver: authentic and secure data that can be trusted as an accurate, factual record of a company's behavior.

**KNOW YOUR CUSTOMER**

Surprisingly, for nearly every business, the public sector is the consumer of the largest volumes of its electronic data. Virtually every aspect of any business is subject to regulations that require data in order for the rule of law to be administered: employment practices, manufacturing practices, accounting practices, fleet maintenance, inventory quality control.
and so on. But most corporate executive teams don’t recognize that new public regulations are intended to better assure that the corporate information systems create and preserve factual records relevant to investigations and enforcement. In other words, each company is required to be the custodian of the data that proves the integrity of its business records.

This is a fundamental shift that has important economic implications. Historically, agencies reacted after the fact: Business records were requested following adverse events that suggested noncompliance had occurred. Companies are now being asked to allow public sector access, sometimes in real time, to ongoing performance data that serves as evidence of compliance. To make that data reliable, agencies are imposing requirements on the systems in which the data is maintained. Spending on e-discovery and lawyers to find records is disappearing rapidly, replaced by front-end information governance investments to ensure data meets public sector demands. And as in all other areas of business, the customer is always right.

These five strategies are being embraced by companies all over the world to secure competitive advantage. They are not easy to implement, but failing to do so could mean costs and expenses that ultimately reduce business value.

—Jeffrey Ritter
As Threats Evolve, Companies Must Re-examine Data Security and Compliance

In the digital age, where cloud usage, bring-your-own-device, Web-enabled applications and big data have become the norm in corporate settings, there are numerous new sources of information risk. Although industry continues to see threats like DDoS attacks that crash systems to make life difficult for system and network administrators, the big draw for hackers continues to be data.

This is evident by many of the largest breaches in the past few years, which often involved data-rich industries such as financial/banking, retail and healthcare. According to Verizon’s 2015 Data Breach Investigation Report, there were significant increases in crimeware use, point-of-sale attacks and incidents using techniques such as RAM scraping—all typically designed to target or steal data. As the threat landscape continues to evolve in response to big data, so have the strategies and technologies designed to keep organizations (and their information) both secure and compliant.

Know your data assets
The first and most important step to data protection in the digital age is to know what information you need to secure. This usually involves three steps: identification (or inventory), classification and tagging.

Identifying data sounds easier than it is, simply because many organizations opt to treat all information equally and implement universal controls across the organization. The practice requires less upfront planning by IT staff, but it can also result in exaggerated security/IT budgets and overworked personnel. A more effective practice is to work with executives and business leaders to identify products and services that are important to the organization. This helps identify sensitive data and the
information that most needs protection. Your legal team should also be consulted, because they know which data types may not have a direct impact on the bottom line but still must be governed properly for compliance purposes.

Numerous technologies are available to help protect and manage data, and they’re even more effective when you have successfully identified and marked the data.

Data classification is an extension of identifying information but goes a bit further to help you organize your data into groups, each of which require unique controls. It also helps establish priorities for particularly sensitive data that should be secured first.

Tagging information or data is often the most difficult of the three processes, considering that not all systems or electronic data lend themselves to being easily marked or labeled. Here are the more common techniques for tagging or labeling data:

- For database records, create fields that can contain a value denoting the type and sensitivity of the data (i.e., a “PCI” field set to “yes” to mark credit card information).

- For flat-file documents such as Word or Excel documents, insert a footer that identifies the type or sensitivity of the data. The footer label could be marked “confidential—financial,” or “restricted—intellectual property,” for example. You could also create corporate boilerplates or master template documents that contain a footer description.

THE DUAL BENEFITS OF DATA PROTECTION TECH
Numerous security technologies are available to help protect and manage data, and they are even more effective when you have successfully identified and marked your data. One of the most common technologies on the market is data loss prevention (DLP) systems.

In most cases, DLP products are installed as a perimeter or “gateway” solution near a company’s Internet ingress/egress points.
Once deployed, most DLP products use pattern-based techniques to monitor content going to or from the Internet, and they even scan network drives or file shares to identify sensitive data at rest on your network. Many DLP solutions include pre-defined “signatures” to help detect common forms of sensitive information such as credit card numbers, Social Security numbers or source code.

Often, DLP systems allow for custom data monitoring techniques that flag data the company identifies as sensitive. Using the custom keyword or code inserted into corporate boilerplates or templates, you can often create search criteria in most DLP systems that will alert you when users are sending data to outside parties without permission. It’s a relatively low-tech tactic but one that is often very effective at preventing corporate documents or intellectual property from being leaked.

Other technology options to consider for protecting your company’s data include the following:

- Encryption or tokenization products to obfuscate the sensitive data from being seen by anyone other than an authorized user.

- Identity management and/or privileged access management to ensure that users/employees don’t have ill-gained access.

- Logging solutions that provide application log analysis for a deeper look at how applications are handling their data.

Data is one of the most important assets a business has in today’s digital world. There are thousands of security products for protecting systems and networks, and the market for products that monitor and secure data is constantly growing. This is largely due to regulations and laws putting more emphasis on data security. The combination of knowing the type of data you need to protect, identifying where it is and implementing specific processes to manage that data will help keep the organization both compliant and secure. —Jeff Jenkins
Mobile Data Security Ambiguity Raises Unique Governance Challenges

**Fairview Health Services** has a pressing need to give its workers access to information wherever they are: If the right data doesn’t get to the right person instantaneously, someone could die, said Barry Caplin, vice president and chief information security official for the Minneapolis-based nonprofit healthcare organization.

To ensure that instant access, Fairview has about 3,500 mobile devices deployed through the organization, including both enterprise-issued and employee-owned devices of various brands and operating systems. The number is growing, as more of its 22,000 employees go mobile.

At the same time, Fairview must contend with the significant security concerns imposed not only by its own data privacy standards but by regulatory privacy requirements such as HIPAA as well. But as the organization’s CISO, Caplin knows that 100% security doesn’t exist.

“The perfect solution would be not to be mobile. But that’s not practical,” he said.

Security and compliance challenges are growing as more employers adopt processes that allow mobile devices to perform work tasks. Workers no longer use devices to just check email and their calendars. As devices are used for increasingly complex processes, data becomes more vulnerable to loss. To keep pace, IT and security executives must develop comprehensive mobile security postures and implement stronger technology solutions.

Unfortunately, that’s easier said than done. That’s because organizations must develop high-level ideas that focus on people and processes first, Caplin said.

“There is a lot in security that’s conceptually simple, but the operational, the boots-on-the-ground stuff is very complex,” Caplin said. “We can’t just slap on a solution because if it
doesn’t mesh with how people work day to day, then it’s not going to work.”

**ESTABLISH APPROPRIATE MOBILE USE**

Caplin has taken a multipronged approach to mobile data protection at Fairview, where clinicians use tablets to share healthcare information with patients and use mobile devices to input clinical data when they visit patients in their homes.

That multipronged approach includes following policies that establish appropriate mobile device data use. For example, employees can’t share patient information via text because it’s unsecured. Employees also receive regular training on these policies.

Caplin uses a virtual interface that keeps the data workers enter onto their computers (whether a desktop or a mobile device) off the actual device. That means, Caplin explained, that if a device gets lost or stolen, there’s no data loss for the organization.

That approach, he admitted, doesn’t work for all his employees, notably the clinicians who provide in-home care. They store data on the devices, which later gets synced, so Caplin layered in encryption, mobile device management, mobile application management and enterprise mobility management tactics.

Despite the trend toward ubiquitous mobility and the growing IT security concerns that come with it, organizations have been slow to adequately address mobile data security. There are various reasons for the trend: Mobile tech advancements put pressure on organizations to adopt them quickly and often without a full security evaluation. Downloading mobile apps without IT approval is also easy and creates plenty of avenues for data to leak.

Then there’s the fact that there has yet to be a major headline-making data breach involving smartphones or tablets.

“It brings the guard down on a lot of enterprises,” Gartner analyst Dionisio Zumerle said.

On the other hand, Zumerle said mobile data security products are maturing as vendors address how to better mesh security measures with user-friendly functionality. Vendors are adding new features such as cloud access security brokers to the market. Organizations are also using advanced IT analytics to detect
anomalies in user behavior that could alert them to vulnerabilities.

**NEW VULNERABILITIES CREATED BY MODERN MOBILITY**

There are certainly plenty of these potential vulnerabilities, according to Nisha Sharma, managing director of mobility at Accenture Digital. Workers could be using apps with little or no security protection, particularly if they’re using apps without any IT review that could introduce malicious code onto their devices. These apps could also be transmitting information on insecure networks.

Then there’s the potential for what Sharma called “data leakage,” where bits of corporate information flow through devices without any corporate knowledge or oversight. These leaks are often through text, screenshots, photos and even audio recordings. Not only do those types of content generally reside in unsecured areas, but IT departments can’t see or track them either, she said.

Getting a grip on how data moves via mobile is a challenge, however, because it’s hard to know how to secure data without visibility.

“IT has no idea that the information is out there on the device,” said Chris Hazelton, research director for enterprise mobility at 451 Research.

Leading executives are working on that, though.

Larry Biagini, CTO at GE, said about half of the company’s 300,000 employees use mobile devices. They use a combination of company- and employee-owned devices, including a mix of tablets, smartphones and smartwatches that run on various *operating systems*.

“Not unlike everybody else, we do use a mobile device management platform, but that’s table stakes. And we don’t believe it’s the ultimate solution,” he said. “We want to understand what devices people have, how they’re

**Workers no longer use devices to just check email. As devices are used for increasingly complex processes, data becomes more vulnerable.**
connecting to our network, what apps they’re running, and we want to be able to wipe them remotely.”

Biagini said GE runs regular training and employee education to keep workers informed of what they should be doing to keep data secure. The company also uses technologies designed to protect data without hindering users. Biagini pointed to the fact that workers can securely access internal GE apps with a simple authentication and without going through a VPN because GE’s systems recognize the device.

“We truly believe that the big piece of the solution we need to provide is an API gateway for all types of applications, so you’re not running apps but making requests for services. That way, we can decide who you are, what device you’re on and where you are in the world,” he added.

The strategy is a good balance between the value of a mobile workforce and reducing the security risks that stem from it, Biagini said. Is it foolproof? No, but as Biagini noted, nothing is when it comes to data security.

“It’s where you put the risk bar, that’s what we have to spend a lot of time on,” he said. “And if we can get visibility [and] know what we want to allow based on our risk bar, we get closer to that balance.” —Mary K. Pratt
**JEFF JENKINS** is a regulatory compliance, information security and risk management expert and currently the director of cybersecurity at Travelport Ltd. Prior to his role with Travelport, Jenkins served in security executive/leadership roles for a number of private and public sector organizations. He currently holds CISSP, CISA, CISM and CGEIT certifications.

**MARY K. PRATT** is an award-winning freelance journalist based in Massachusetts. Her work has appeared in numerous publications, including newspapers, magazines and trade journals. She currently focuses her coverage on business management and information technology topics.

**JEFFREY RITTER** is one of the nation’s experts in the converging complexity of information governance, security and the use of digital information as evidence. He advises companies and governments on successful 21st-century strategies for managing digital information. He is currently developing and teaching courses at Johns Hopkins University’s Whiting School of Engineering and Georgetown University Law Center.