KnowBe4
Human error. Conquered.

THE CHALLENGE OF THIRD-PARTY COMPLIANCE MANAGEMENT

Overcoming the Challenges of Managing Third-Party Compliance With Data Protection Laws

WHITEPAPER: The Challenge of Third-Party Compliance Management

Table of Contents

Data Privacy & Security Laws Are Multiplying 2

Third-Party Compliance and Risk Management 3

Signs of Poor Vendor Compliance Management 4

Decentralized Authority 4

No Data and Process Inventories 5

Inefficient Tools 5

Lack of Automation 5

Conclusion 5

KnowBe4’s KCM GRC Platform 6

Additional Resources 6

Three Misconceptions 7

What to Ask Your Third-Party Providers 7

How Mature is Your Third-Party Management Program? 8

DATA PRIVACY & SECURITY LAWS ARE MULTIPLYING

Cyber crime and data theft have increased substantially over the past few years, and so have government efforts to protect data with tighter privacy and security laws. Data breaches, identity theft, and financial fraud are growing, global problems. *Risk Based Security's Cyber Risk Analytics 2019 MidYear QuickView Data Breach Report* counted 3,813 data breaches during the first half of 2019, which exposed more than 4.1 billion records including birthdates, bank account information, and social security numbers. That number is 54% higher than 2018's mid-year count—and it only includes publicly-reported break-ins.[1]

In response, several countries are increasingly regulating how organizations protect sensitive data. One or more data protection laws cover most organizations, depending on the type of data they collect and where they do business. For instance, any organization that has personal data on a resident of the European Union (EU) must comply with the EU's General Data Protection Regulation (GDPR). That includes even small ecommerce companies if they sell to EU consumers. Other countries, such as Canada, Germany, Japan, the U.K., Argentina, and South Africa, have enacted their own consumer data privacy laws.

While the U.S. lacks a universal federal law on data protection, many states and industries have regulations. For instance, the U.S. Family Educational Rights and Privacy Act covers colleges and universities. The Sarbanes-Oxley Act, which enforces cybersecurity on financial records, covers public companies. Banks must comply with the Gramm-Leach-Bliley Act to protect consumer data. And any organization that accepts credit card payments must comply with the Payment Card Industry's Data Security Standard (PCI-DSS).

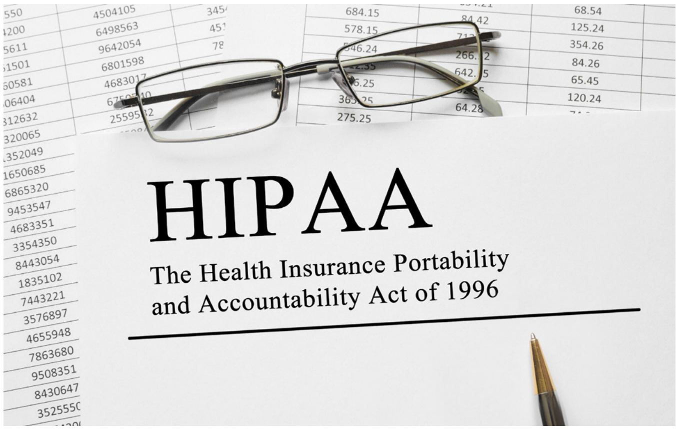
At least 25 U.S. states have enacted consumer data protection laws. The newest is California's Consumer Privacy Act which, as of January 2020, requires companies and their trading partners to provide consumers access to their own personal data and to delete it upon request.

Non-compliance with these various regulations can result in penalties, as well as loss of business and possible lawsuits in the event of a data breach. Organizations that fail to comply with PCI-DSS may face a fine of up to $100,000 per month of non-compliance.

Cyber criminals are getting ever smarter at hacking into IT systems and stealing sensitive data. As data breaches increase and online fraud grows, so does the importance of complying with local, national, and international regulations on data security and privacy. Every organization, whether a for-profit business, non-profit association or government agency, must ensure that its data is handled according to the law—both internally and when the data is shared with third-party providers.

[1] Risk Based Security's *Cyber Risk Analytics 2019 MidYear QuickView Data Breach Report*

That’s not significant for a large company but may be serious money for a small- or medium-sized business. Worse, non-compliance may revoke the company’s right to accept credit card payments or cost the company more in banking fees.


HIPAA
The Health Insurance Portability and Accountability Act of 1996

Other regulations carry stiffer penalties. Cottage Health, a regional hospital chain in California, fell afoul of the Health Insurance Portability and Accountability Act (HIPAA) for two incidents that exposed sensitive patient data. The company was fined $3 million by the U.S. Department of Health and Human Services.

GDPR carries the most severe penalties, ranging from 2% to 4% of revenues. British Airways was assessed a fine of $230 million when its web site traffic was hacked and redirected to a fraudulent site that collected customer credit card numbers and other data.

Complying with this growing collection of international, national, and state regulations is a major challenge for small and mid-sized organizations that lack the necessary expertise and resources. The compliance management process includes a long list of responsibilities such as:

- Creating internal compliance policies
- Providing security and privacy awareness training to employees
- Tracking and investigating issues
- Keeping up to date on changing regulations and new regulations
- Documenting compliance and providing visibility into the data for auditors

THIRD-PARTY COMPLIANCE AND RISK MANAGEMENT

Every organization today has multiple partners—suppliers, service providers, staffing agencies, IT consultants, marketing agencies—with which they share data or access to their computer systems. A 2019 survey found 44% of companies experienced a significant data breach caused by a third-party vendor.[2]

Any organization that provides a third party with regulated data or access to IT systems that contain the data is responsible for that third party’s compliance and could be penalized if the data is lost or leaked.

Ensuring the compliance of dozens, or even hundreds, of outside companies is a daunting task for any organization but especially for small- and mid-sized ones that lack adequate resources. Third-party compliance management includes time-consuming activities, including the following:

- Develop, distribute, and collate responses to questionnaires to assess third-party data security and compliance
- Review assessments of third-party security and privacy to identify issues
- Communicate with internal departments that own the relationship with each third party
- Manage the large number of documents needed for audits
- Conduct third-party risk assessments

[2] HelpNetSecurity, *Nearly Half of Firms Suffer Data Breaches at Hands of Vendors*

TPRM (Third Party Risk Management) is the process of identifying and controlling the risks that a third party's non-compliance poses to an organization. What are the risks of doing business with it? TPRM evaluates and manages those risks.

TPRM includes evaluating companies based on a list of weighted criteria. The vendor then typically is given the opportunity to resolve issues and reduce its risk to the evaluating organization. A high-risk vendor may require additional follow-up or, in worst cases, the relationship may be severed.

Organizations serious about data protection and compliance can't afford to do business with high-risk partners.

SIGNS OF POOR VENDOR COMPLIANCE MANAGEMENT

Third-party, or partner, compliance management is an extension of an organization's internal compliance management. Inadequate internal compliance practices inevitably lead to poor third-party compliance management.

Following are the major warning signs that an organization needs to improve its compliance practices, both internally and with third parties.

Decentralized Authority

In organizations that lack a compliance manager, individual departments may have to handle compliance for their own data and third-party relationships. Marketing might have to document how it shares customer data with its marketing agency, for instance. Human resources may be responsible for ensuring compliance of employee data that goes to an insurance provider. A 2018 Osterman Research Inc. report for Knowbe4[3] found that more than one-quarter of the organizations surveyed have at least six people involved in compliance tasks, while 7% have more than 20 people involved. A decentralized approach can lead to disorganized and inconsistent compliance processes, with incomplete, scattered documentation.

While department staff should be involved in compliance, centralization can ensure the integrity and completeness of documentation and the consistency of practices and policies for the entire organization.

[3] Osterman Research, *The Critical Need to Improve Compliance Processes*, 2018

No Data and Process Inventories

Compliance requires knowing what data is flowing out of your organization and to your suppliers. That means maintaining an inventory of the organization's regulated data, such as social security numbers, employee health insurance data, financial information or other personal identifiable information (PII). A data inventory may include information about the data, such as the level of sensitivity (e.g., public, internal use only or sensitive), the data's owner, and the third parties that share the data.

Another necessary inventory is the data process inventory, also called a data flow map, which documents the processes used to gather and share data. An example might be a payroll process in which employee addresses, social security numbers, and salaries flow through human resources and finance out to the payroll processor. The lead generation process is another example. How is consumer data collected, where does it go, and how is it stored?

Inventories can be created manually, but that is an inefficient and time-consuming method. Many software applications on the market today automate data discovery and mapping.

Inefficient Tools

The Osterman Research report found that 62% of respondents used spreadsheets as their main compliance tools. Many organizations said they were unaware of other compliance solutions or lacked the funds to purchase one. Organizations that use spreadsheets must laboriously input large amounts of information by hand. That data includes:

- Data inventories
- Vendor contacts and ratings
- Compliance issues and updates
- Compliance regulations and requirements
- That amount of manual data input represents a lot of wasted productivity and potential for error.

Lack of Automation

Organizations that use spreadsheets for compliance have a related problem—lack of automation of the compliance process. Compliance management involves many processes, most of which can be done quickly and efficiently through automation. Automating the workflow not only saves employees hours of manual labor, but ensures that critical due dates and reminders aren't forgotten.

For example, an automated process can check for changes to data protection laws and update a database of regulations and requirements. Or it might automatically email monthly reminders to vendors to update their compliance documentation. Automation can save time and staffing costs, as well as reduce human errors.

CONCLUSION

Managing an organization's compliance with international, national, and state laws is an enormous responsibility. But the costs of not complying can include six-figure (or higher) fines, legal action, negative publicity, brand damage, and loss of business. Unfortunately, as the regulatory landscape for data privacy and security laws becomes more complex, many organizations lack the resources to conduct a compliance program. Many small- and mid-sized lack even basic knowledge of the laws that apply to their data, as well as the staff and software tools to do the job correctly.

However, they can improve their compliance significantly by adopting a compliance management solution to automate processes and tasks to reduce the burden on employees. Rising awareness of the need for better data protection has expanded the number of affordable compliance management applications, many of which include automated workflows, templates for various regulations, customizable vendor questionnaires, and third-party risk management. With the right tools, organizations can greatly improve their internal and third-party compliance management.

KnowBe4's KCM GRC Platform

Most old-school, on-premise compliance applications require months of implementation and outside consulting help to deploy, as well as a commitment to yearly maintenance and support fees. Small, mid-sized organizations, and many divisions of multi-nationals can't afford this high cost, nor do they need an enterprise compliance platform. There are affordable, cloud-based alternatives, however. KnowBe4's KCM GRC application has a simple, intuitive user interface, easy to understand workflows, a short learning curve, and deployment that takes days, not weeks or months. It's also affordable for any size company. KCM GRC makes it easy to get rid of spreadsheets and manual processes and efficiently manage risk and compliance both internally and for third-party providers.

Organizations worldwide use KnowBe4's software across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

For more information, please visit www.KnowBe4.com, Sales@KnowBe4.com, 855-KNOWBE4 (566-9234)

Additional Resources

- Osterman Research and Knowbe4, *The Critical Need to Improve Compliance Practices*
- *Costs of Non-Compliance with Privacy Laws*, September 2019
- CIOReview, *Enhancing Compliance Automation Efforts Step-by-Step*, Amy Matsuo, Principal, global leader for compliance transformation solutions, KPMG and Todd Semanco, partner, banking and consumer compliance risk, KPMG
- Shared Assessments and Protiviti, *2019 Vendor Risk Management Benchmark Study: Running Hard to Stay in Place*
- KnowBe4, *Improving Legal Compliance Through Security Awareness Training*
- KnowBe4's *KCM GRC Platform*

THREE MISCONCEPTIONS

Without the time or resources to hire a compliance expert or invest in compliance management software, smaller organizations may not fully understand how compliance works. They often have misconceptions as to what constitutes compliance or who's responsible for it. Three examples:

1 One misconception is that organizations aren't responsible for how third parties handle their data. An organization is responsible for its data even after it passes outside the company to a third-party supplier or, even, a fourth party.

2 Another misconception is that effective cyber security technologies ensure legal compliance with data protection laws. Unfortunately, that is not true. Cyber security technologies certainly help protect against a data breach and enhance its odds of complying. However, your organization may have the most advanced security technologies and still not comply with some aspects of a law or regulation, such as privacy protections or data sharing practices.

3 Finally, many SMBs believe that moving data and applications to the cloud transfers the responsibility for compliance to the cloud provider. While a cloud provider's security may fulfill compliance requirements, it's not guaranteed. Cloud providers that have passed a System and Organization Controls (SOC) 2 audit are certified as having met requirements for data security, availability, and processing integrity. However, that doesn't mean they're ultimately, legally responsible for their customers' data security. Most service level agreements (SLAs) for cloud services spell out who is responsible for different types of security (e.g., facility security or Azure platform security). The client is almost always responsible for ensuring the security of their own data.

WHAT TO ASK YOUR THIRD-PARTY PROVIDERS

Assessing third-party risk starts with a vendor questionnaire. Some compliance applications, such as KnowBe4's GRC application, have customizable questionnaires and automated online processes to make completing and assessing them easier. Whether automated or manual, however, a list of questions for a third-party evaluation might include the following:

- Has the third party recently passed a compliance audit? Were all recommendations for improvement implemented?
- Does it have a formal data security policy? Is it updated at least annually?
- Do their employees receive security awareness training? At least annually?
- Are passwords managed according to best practices?
- Do their employees use instant messaging, and if so, is it secured using reasonable best practices?
- Does the third party have a documented breach response plan? Is it updated at least annually?
- Has the third party implemented cybersecurity defenses in line with their data security policy and known risks?

HOW MATURE IS YOUR THIRD-PARTY MANAGEMENT PROGRAM?

How sophisticated is your organization's third-party compliance practices? Companies that have mature compliance programs can answer "yes" to these ten questions:

✓ Do you maintain an accurate inventory of vendors?

✓ Do you identify criticality of vendors?

✓ Do you have established staff responsible for evaluation of vendors?

✓ Do you evaluate vendors differently based on the type of data they have access to?

✓ Do you know what vendors have access to each class of data?

✓ Do you have standardized assessment questionnaires to evaluate vendors?

✓ Do you establish schedules to periodically reevaluate vendors?

✓ Do you communicate with vendor stakeholders?

✓ Do you have a remediation and risk acceptance process for vendors?

✓ Do you have a process to deprovision vendors after contract expiration?

If you got a 10, congratulations! You're doing great. If you scored a 7 or higher, you're doing well…just a little more work. If you got a 5 or 6, you're heading in the right direction, but need improvement. If your program got a 4 or under, sorry but you need some help!

Start by reading the *KnowBe4 Compliance Blog*, then visit the *KnowBe4 KCM GRC* site to learn how an automated compliance application can help.

Additional Resources

Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make better security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com