Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Adopting Effective Data Privacy Controls

COMPLIANCE WEEK

Compliance Week, published by Wilmington Group plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resources for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

Information in this book is intended for public discussion and educational purposes only. It does not constitute legal advice and does not create any attorney-client relationship with the author.

Table of Contents

Assessing your Digital Marketing Risk

by Tammy Whitehouse
January 21st, 2015

Cyber-security is taking a new twist in 2015 as companies begin to assess risks posed by sales and marketing activities that rely on digital channels and social media.

Long gone is the deliberate pace of marketing from the "Mad Men" era, where teams took days or more to mock up proposed print advertising that went through multiple layers of review. Digital marketing moves more quickly, involves more people, can trigger more regulatory oversight, and is far more prone to fraud or data theft than anything Don Draper worried about.

Little surprise, then, that Corporate Executive Board lists digital marketing as a "hot spot" in internal audit planning that deserves greater corporate attention in 2015. The rise in digital marketing gives companies the ability as never before to target their sales and marketing activities to specific customers. But it also produces reputational and data privacy risks playing out in news headlines with greater frequency, CEB says.

"This is something many internal auditors are not familiar with," says Ruth Shaikh, associate director at CEB who performed the research that led to CEB's conclusions. "When we talk about digital marketing, we mean use by companies of digital channels—like social media, e-mail, Web applications—to connect with their customers and stakeholders." The idea that digital marketing channels can create risk is perhaps not news to internal auditors, she says. Knowing how those risks are created, and what controls should be in place to mitigate them, is a work in progress.

> "When we talk about digital marketing, we mean use by companies of digital channels—like social media, e-mail, Web applications—to connect with their customers and stakeholders."
>
> Ruth Shaikh, Associate Director, CEB

The potential risks are every bit as numerous and complex as the modern digital supply chain and its long list of characters, says Danielle Ritter, assurance director for PwC who works primarily in technology and media sectors. "If you're sharing data, what are you sharing?" she asks. "Who are the partners you're working with? Who is helping you deliver or build your digital marketing campaign? Internal auditors may want to evaluate the risks of those parties." That's a key part of protecting the data the company is sharing with its service providers, she says.

Digital marketing fraud is rampant, says Linda Wooley, president and CEO of Trustworthy Accountability Group, a grassroots organization trying to combat the problem and give companies standards and tools to protect themselves. "The entire supply chain is very complicated, with a lot of parties in the chain to deliver a digital ad," she says.

The supply chain even for something as simple as an online advertisement has advertisers, ad agencies, ad buyers, advertising networks, ad exchanges, publishers, and auctions to bid for ad dollars and placements. Along the way, nefarious players sneak into the system and siphon off ad dollars that never deliver the advertising impressions intended, she says.

Another risk, Wooley says, is piracy: rogue players picking off legitimate ads and creating spoofs re-directed to fraudulent URLs. "It looks as if those ads appeared somewhere, so the criminals are paid, but the ad was not seen by a human," she says. "And there are many, many more types of fraud in the system."

The Association of National Advertisers recently released a study showing that advertisers will lose $6.3 billion of their advertising spend globally in 2015 to non-human bot traffic. The scam is that "clicks" on online advertisements are made by machines with no actual spending power, rather than humans that the advertisers were paying to get. For U.S. companies, that amounts to as much as 30 to 50 percent of a company's digital advertising budget, Wooley says.

"So you have chief marketing officers looking at their budget and saying 30 to 50 percent of what I spend on digital advertising is wasted," she says. "That's not sustainable."

Getting Ahead of the Problem

TAG is in the early stages of creating standards for participants in the digital advertising supply chain, intended to reduce the ability of illegitimate players to weasel their way in. Such standards will be helpful not only to advertising and sales executives, but to internal auditors as well, she says. "There will be business rules for everybody who operates in the ecosystem. These will be things you need to do to vet your vendors."

The role of internal auditors is to get educated on digital marketing risks and help manage those risks across the enterprises, Ritter says. "Digital marketing is a relatively new area of risk, and it's constantly changing," she says. "You don't always see marketing and advertising as a high focus in the internal audit plan, but companies should start by inventorying what their digital marketing touch is."

Bill Michalisin, chief marketing officer for the Institute of Internal Auditors, says internal audit's focus so far for digital marketing risks has centered on the employee side, or what companies are doing internally. "Now we're seeing more instances of social hijacking, more cases where parties outside are coming in and doing damage," he says. "Companies haven't viewed it that way very much."

Interest in more education and information on digital marketing risks is growing in internal audit circles, Michalisin says. "It's a newer area, so I don't know if we can say there are even best practices yet per se," he says. "There is a need for peers to share ideas and strategies they can start to put into place to address this. There is demand for that."

He suggests internal auditors start the dialogue within their own organizations to assess the company's exposure as a result of its digital marketing activities. "Once internal audit has a full view, they can bring to the conversation their expertise and their perspective around mitigating risks and evaluating controls."

Warren Stippich, a partner and national GRC leader for audit firm Grant Thornton, says larger companies that are brand-driven and consumer-oriented generally are further along the learning curve in assessing and responding to digital marketing risks, but virtually any company could benefit from reviewing their policies and procedures. Before digital, sales, and marketing activities generally were subject to layers of internal approval before anything would be released to the public, he says.

"Now, anyone can upload and hit 'post,' and it happens in seconds, read by tens of thousands of constituents," he says. "That's a big risk."

CCOs Playing a Stronger Role in Data Privacy Practices

by Aarti Maharaj

August 11th, 2015

As data privacy laws proliferate around the world, they are creating a web that traps how corporations use personal data in their operations. The challenge for compliance officers: how to play a more strategic role in the organization, ensuring your business doesn't get stuck.

So far that effort hasn't been easy. In the Compliance Trends 2015 report published by Compliance Week and Deloitte, 59 percent of compliance officers are either "somewhat confident" or "not confident at all" that their IT systems can fulfill the data collection and reporting requirements they have. That can cause problems in how your business gathers data, how it uses data, and even how the business recovers from regulatory and reputation risks when it loses data, through hackers or otherwise.

> "Technology is its own discipline and I don't see compliance officers becoming technologists overnight."
>
> Todd Cipperman, Principal, Cipperman Compliance Services

"The issue for chief compliance officers is that they are increasingly struggling to connect regulatory requirements to IT issues," says Todd Cipperman, founding principal of Cipperman Compliance Services. "Technology is its own discipline and I don't see compliance officers becoming technologists overnight."

The forward march of technology—specifically, data storage in the cloud—does chief compliance officers few favors. According to research firm Gartner, by 2017 50 percent of an organization's business data will reside outside the physical walls of your corporate data center, up from less than 10 percent today. According to Eurostat, the statistical office of the European Union, about 20 percent of enterprises will rely on cloud computing across the Organization for Economic Co-operation and Development. (Finland is currently leading the race at 50 percent, Poland in the rear at 6 percent.)

The problem is that few compliance officers are involved in high-level discussions around cloud computing and data privacy controls, which can be disastrous for companies as they expand into new locations.

"Employee data is becoming something on the forefront of compliance," says Marie Blake, executive vice president and chief compliance officer at BankUnited N.A. "To avoid an in-house privacy breach, you have to think about what is included in privacy data, like information governance, and you have to move with the direction of the industry."

Currently the industry is moving to play catch up with the risk. One example is the massive breach of financial institutions at JPMorgan and several other large banks last year, where prosecutors and IT security reportedly are still sizing up exactly how the attacks happened and how widespread the damage was (tens of millions of customer records, at least).

IT security tools will help that threat, but often tools address one specific risk. If the process for governing information is weak overall, that leaves the company exposed to any number of other risks your IT security tools don't address. And the moves in Europe and elsewhere around the world to strengthen data privacy laws makes that need for information governance all the more acute.

"From a compliance perspective you want to put policies in place to defend a claim," Cipperman says. "This is sometimes hard for compliance officers to do because it's not easy to understand what are the data security operations in place."

Pressure on CCOs

The CCO mandate is to be aware of and ensure their organization adheres to the laws and regulations relevant to their business. Therefore they should absolutely be at the table for discussions around technology," says Janet de Guzman, director of compliance at OpenText, an enterprise information management firm. "Data and privacy protection is becoming a critical part of the compliance function because it's not only their own data at stake but the data of their customers and other stakeholders."

Blake says that not many CCOs are involved in their companies' data privacy committees, and she expects that to change over time as companies realize that CCOs bring critical knowledge about regulatory requirements to their cyber-security discussions.

"The inclusion of the CCO function in defining controls related to things like cloud computing has yet to hit maturity," Blake said. She compared it to vendor management, where initially compliance officers were not involved but are now vital voices at the table. (Think of all the trouble third parties can bring to your business.)

"I see that evolution in the information security and data protection space as well," Blake says. "It's simply a matter of time for banks to further include the CCO into that realm of information governance."

Ground Zero for privacy regulations complicating business operations is, of course, France. French data protection laws date back to the 1970s, and the tough stance of the Commission Nationale de l'Informatique et des Libertés, its data protection authority, has flummoxed many U.S. businesses. In 2014, CNIL fined Google €150,000 ($164,000) for changes the company made to its privacy policies.

The enforcement was triggered by an announcement that Google planned to replace product-specific privacy policies with single, overarching terms without notifying users ahead of time. An investigation by the Article 29 Working Party, an advisory body comprised of DPAs from 28 European member states, ruled that Google's privacy policy violated the European Data Privacy Directive because users were not informed of what data would be collected, or why, and data retention timelines were not public.

Regulatory skirmishes like that will force companies to consider data privacy compliance more seriously as they plot business moves. Europe is simply the biggest example, not the only one.

"The data security laws in the EU are complex, with non-EU countries beginning to follow suit," says Meena Elliot, chief legal officer at Aviat Networks, a $350 million maker of wireless transmission systems. "Google is facing challenges concerning the EU's views on the right to be forgotten from the Web. At the moment, there is no such requirement in the United States."

> "Google is facing challenges concerning the EU's views on the right to be forgotten from the Web. At the moment, there is no such requirement in the United States."
>
> Meena Elliot, Chief Legal Officer, Aviat Networks

But Google has been facing intense heat, especially from France. Recently the company received a formal notice from CNIL calling for Google to delist links from all European versions of Google Search and all global versions as well.

In response, Google argues that while European law enforces the right to be forgotten, its scope is limited and can't be applied globally. In fact, content (read: data) that is illegal in one country may be legal in another—one more challenge that companies face as they grapple with data privacy compliance.

"Google's stance in this case means a lot for compliance officers, and it serves as a warning for companies as they expand into new regions," de Guzman says. "It shows that the chief compliance officer constantly needs to be aware of new legal developments and have strong policies in place as governments around the world roll out new or more stringent data privacy laws."

"The compliance function has dramatically evolved over the years," Blake says. "Now we are engaging more in IT solutions that help to protect customer information. Although the functions between compliance, IT, and information security are still somewhat separated, we work very closely with these areas to have a sense of the overall controls in place to protect consumer and employee data."

Clouds With Industry-Specific Compliance Built In

by Todd Neff

March 19th, 2013

The arguments for industry-specific cloud computing are becoming more compelling.

Take the pay-as-you-go cost advantages and expand-as-you-need flexibility the cloud affords, and add layers of industry-specific processing, security, and compliance. Indeed, ever since a couple of high-profile industry-specific cloud providers emerged in 2011, such as the NYSE Technologies' Capital Markets Community Platform and SITA's ATI Cloud for the air-transport industry, industry-specific clouds –also known as community clouds–have continued to proliferate.

But it has been quieter than was the case with the initial pulse of public cloud uptake few years ago, said David Linthicum, an independent cloud consultant and InfoWorld blogger. He suspects there's a reason for that. "At the end of the day, we're building what are in essence enterprise applications, just in a way that can be consumed over the Internet, and I think people are realizing it's no big whoop."

So they're not tabloid fodder. But community cloud offerings do offer things a public cloud can't, not least of which is to handle tough industry-specific security and compliance requirements. As Mark Wright, NYSE Technologies' vice president of product management put it, "We take great pride in being a very un-public cloud." Community clouds like that of NYSE Technologies come with assurances that cloud-stored data will remain safely in a specific country, region, or even data center. They are housed either in private clouds—server farms owned and controlled by the entity offering the community cloud service—or they provide secure gateways into the clouds of hired-gun providers. And they are often tailored to satisfy specific, existing business needs.

Nasdaq OMX's FinQloud is one example. FinQloud's main pitch is dealing with SEC 17a-4 record retention rules. Rather than securities broker-dealers having to store seven years of transaction data, they can send it off to FinQloud. Customers enter through a secure NASDAQ gateway, and NASDAQ servers hold the encryption keys. But the data itself resides on the Amazon Web Services cloud. NASDAQ officials say the service saves clients 80 percent in data-storage costs.

Compliance issues have pushed financial industry-specific cloud far from the fingers of the public Web, says Alex Tabb, a partner with capital markets research and advisory firm Tabb Group.

"They are for all intents and purposes segregated from the rest of society—no one in capital markets is going to put this kind of important, very strategic, confidential information anywhere near where people can get access to it," Tabb says. Compliance issues, he adds, remain a top concern among financial players looking at any sort of cloud solution.

> "At the end of the day, we're building what are in essence enterprise applications, just in a way that can be consumed over the Internet, and I think people are realizing it's no big whoop."
>
> David Linthicum, Consultant and InfoWorld blogger

NYSE Technologies' Community Platform resides entirely in the secure confines of NYSE data centers, in which clients have been comfortable for decades. Once inside, investment banks can crank out regulatory reports, hedge funds can test and validate strategies, and financial firms of all sizes can test custom applications.

Wright says customers are looking for a range of services. Some seek straight infrastructure as a service (Iaas) on which to set up their own private clouds. Others make use of software bundles NYSE has developed to quickly build out, say, a new trading solution. Others focus on disaster recovery, or communications compliance, or SEC 17a-4 record storage, he says. Client firms may still be wary of a wholesale outsourcing of their servers, Wright says, but for things like record retention, "Can you unload that for me?" is a common refrain.

The list of financial industry cloud players is growing—Bloomberg Vault and Thomson Reuters Elektron being among the notable entrants. Linthicum says he's consulting with several financial firms developing community cloud services. Part of the challenge for community cloud shoppers, Tabb says, is figuring out which service best aligns with their goals. Smaller firms are paying close attention to community clouds, he says, seeing them "as a way of getting away from the very expensive infrastructure they need —they can just go to the cloud and pay based on what they use."

But bigger players are just as interested, Wright says. "There's a trend toward bigger shops and more aggressive moves," he says. "Clients have known for years that they need to rethink their cost structure. They need to consider managed services more broadly. What can they push out of their shop to save money? They can't do it all themselves."

The Nasdaq OMX model of picking a specific battle represents a common community cloud theme, says Mike West, vice president at distinguished analyst at Saugatuck Technology.

He cites the example of Pixar's RenderMan On Demand cloud offering. Rendering digital animation is processing intensive, the costs of high-end servers contrasting with the "feast or famine" nature of filmmaking. IGT Cloud is another example of cloud-based software as a service (SaaS). It gives casino operators cloud-based access to hundreds of games in IGT's game library.

"Here's a model that I think makes a lot of sense for a lot of industries," says West.

Community clouds could make themselves attractive in other ways. There could be community cloud platforms that help retailers develop PCI- and financial-regulation-compliant systems, including shared databases for things like fraud detection, West says.

So where else are these community clouds? The financial industry is the hotbed, Linthicum says, but healthcare players are also increasingly interested. "Manufacturing doesn't have the money. Retail doesn't have the money," he says. "I think healthcare really doesn't have the money, but they have to do it to survive."

Easing the Transition

Transitioning to the cloud can be tough for these institutions, though. While cloud-based options like CareCloud and Optum Health Care Cloud exist, an institution may be running a major electronic health record like Meditech or Epic in-house in addition to multiple tangential systems and data warehouses.

"That's kind of the untold story in the cloud world," Linthicum says. "Most are pushing back on the cloud not because it's too risky or because of compliance issues, but they don't have the money."

Community clouds are also a hot topic among governments, particularly now that one of the biggest compliance-related issues has been removed from the equation, says Brian Bodor, a partner with law firm Pillsbury Winthrop Shaw Pittman in Washington D.C.

Amazon's GovCloud and others have found ways to ensure that government data stays in the United States, Bodor says. In Amazon's case, the offering also meets federal encryption requirements and complies with U.S. International Traffic in Arms Regulation (ITAR) requirements. That's good news for governments and agencies facing budget shortfalls and for whom capital investment is often trickier to budget than operating expenses, he adds.

"What makes the cloud attractive is that it's more a utility model," Bodor says. "It has the potential to bring costs down dramatically."

Data Governance 101: Getting Started

by Joe Mont
April 14th, 2015

Data fuels modern business, but ensuring the quality, usability, and profitability of all that information remains a struggle. And not only does the use of that data need to obey ever-expanding regulatory demands and privacy laws; it should also help alert a business when an employee, unit, or supplier poses a risk.

That's a pretty tall order, then, for good data governance.

"The only good data that is worth investing in is the information that creates greater velocity in the way you make business decisions," says Jeffrey Ritter, a technology consultant and lecturer at Georgetown University's Law Center. "There is tons of data being collected. What businesses need is more information that is trusted and immediately accessible."

The concept of data governance—establishing internal controls, protocols, and procedures to ensure that data assets are managed well—is nothing new. In fact, many describe the current iteration of these protocols as "data governance 2.0," a term that encompasses the explosion of Big Data and its associated analytics. The truth, experts say, is that companies of all sizes, in all sectors, have plenty of work to do.

"Across the industry we are playing data defense," says Alan Paris, global head of financial services consulting for eClerx, a global technology company. "How do you transform that into data offense? How do you actually monetize data? How do you use the approach that you take to data, data management, and data governance to drive business? There is a lot of wood to chop there, and a lot of opportunity yet to be mined."

> "Traditionally the hardest problems to solve are the ones that are not solved in a single line of business or in a single workflow."
>
> Harald Collet, Global Head, Bloomberg Vault

"With all of the competitive pressures that are on companies today, they can't afford not to know that the information is accurate," Ritter says. "They can't process fiction." Likewise, there must be assurances that the information can be used and analyzed without violating any regulatory obligations tied to the data. In privacy law, for example rules pertaining to personal information limit the use of that data. "That's important to the compliance community because their job is to align those rules of use to information assets," he says.

To understand what must go into a data governance initiative, think of it as an e-discovery program on steroids. The first objective is to make sure you know what data you have and that you can easily catalog and access it. Taking that inventory, however, cannot be offloaded to the IT department, since the business units are in the best position to know the data they need and the risks (regulatory or otherwise) that they face.

Protocols to govern data should be developed through a cooperative effort that includes management, compliance, and legal. "Traditionally the hardest problems to solve are the ones that are not solved in a single line of business or in a single workflow," says Harald Collet, global head of Bloomberg Vault. "You need a strong-willed and forceful leader, because there are a lot of obstacles to getting five or seven different parts of the company all on the same page."

"You need executive buy-in and support," says Rex Ahlstrom, chief strategy officer for BackOffice Associates, a data governance consultant. "How high up the food chain can you get? That will depend on a company. Maybe it's the VP running a division or the CIO, but somewhere along the line you need the buy-in."

Put to rest the notion you can just plug in a solution. "You can't just buy it," Ahlstrom says. "It needs to be a combination of the new processes you will have to implement, tying it into business value, and creating the right reporting structure so you can demonstrate a return and expand. You can't solve this with technology alone. You have to start with the right people, the right processes, and the right organizational structure."

Business owners "know what that data is used for and where it gets leveraged when they run those business processes," Ahlstrom adds. "If business is not a stakeholder and owns this, IT really has no idea where to go or what to do." He points to a Gartner statistic that shows how companies might bridge the gap between IT and the business: The research firm predicts that by 2017, 50 percent of companies will have a chief data officer.

Collet's advice is to avoid the temptation to "attempt data governance across the entire company." Instead, narrow the scope of the implementation by focusing on the most regulated line of business.

Small Bites

Breaking the task into steps will also help navigate the complex world of data privacy laws. "You have to implement a data governance solution, but unfortunately you can't move the data into any kind of central place because of the data privacy rules in other countries," he says. "You can end up in a stasis of not being able to do anything because of all the risks that operations, compliance, or legal teams see."

By prioritizing efforts within specific geographies that are less challenging, a data governance program can still gain momentum. "You need to set a strong business strategy so that instead of worrying about all the risks and unknowns, you make intelligent tradeoffs between a business strategy and the risks that are involved in deploying solutions in a certain way," Collet says.

"Certainly there is a strong cyber-security mandate now," he adds. "You have to get your house in order and know what data you have in order to protect it."

"Getting your data act together is paramount to avoid steep fines, reputational risk, and embarrassment," Paris says. "The stick is the regulatory fines you want to avoid by getting your data act together. Then, there is the carrot where you can actually run a more efficient and less capital-intensive, less costly business environment."

A data governance program needs to ensure data quality, accuracy, and reliability. "You have to fix the data at the source and you can drive accountability by creating scorecards and rating people for, essentially, their data citizenship," Paris says.

Some, he says, are considering whether to factor those goals into compensation. "So, if you are a bad actor and consistently providing poor, unclean, or spotty data to the rest of the organization, that's going to affect your paycheck," he says. "Managing compensation is a very good way to manage behavior and provide the proper incentives."

Just as company websites can mine a wealth of relevant customer data, social media can also be ripe with helpful information, including insight into customer behaviors and buying patterns. A company can assess its reputation, see whether marketing efforts resonate, and even pick up on inadvertent pricing and labeling issues. The challenge, as it is with other data streams, is separating good data from the bad, and that is easier said than done, given the sprawling nature of social media sites.

"Social is an interesting data source that presents interesting problems," Collet says. He suggests that it be viewed as a subset of the company's overall approach to collaboration data and use of services like Yammer, Salesforce Chatter, Bloomberg terminals, and other communication channels.

"Social media seems different, and can be very fragmented, but what you want to do from an enterprise data management perspective is not treat it as something that is very different," he says. "Treat it just as you would your e-mail system or an instant message sent inside the company. Then you can start getting consistency across the channels and a 360-degree view of the interactions."

Privacy Compliance Programs: What the Data Really Says

by Matt Kelly

August 4th, 2014

Hand-wringing about privacy and cyber-security is all the rage in corporate governance and regulatory circles these days. So I was delighted when NERA Economic Consulting published a research paper recently asking a long-overdue question: Exactly how much is privacy worth to consumers, anyway?

The research on this point is scarce—which is startling, since companies devote so much time to devising privacy compliance programs and defending themselves in court when those programs don't work. Then come the bad publicity, the unhappy board, and, ultimately, compliance officers sweating out yet another review of breach-disclosure protocols, IT security controls, and data collection policies the marketing department adopted without telling anyone.

All of that rests on the premise that companies must protect personal data because personal data has value. So how much value are we talking about? A lot, apparently.

NERA devised a test asking consumers to select an online video streaming service. Test subjects had to choose one package from a number of possible choices, each one offering various degrees of privacy: an expensive package that shared no data with third parties; a mid-price package that shared your viewing habits but not your personally identifiable details; or a cheap package that shared both.

The study found that test subjects preferred video packages that did not share any data about them, a conclusion so obvious it should surprise nobody. More interesting was this: that consumers were also willing to pay considerably more for packages that shared less of their data. I'll skip the statistical analysis here (it's in the NERA paper if you like), but the test packages were priced from $6.99 to $12.99, and NERA calculated a privacy "willingness to pay" factor of $6.01—an exorbitant amount for products in that price range. Or as NERA put it, "This suggests that consumers care a great deal about privacy and would be willing to pay a substantial fee to avoid sharing their information with third parties."

Compliance officers should draft strong privacy policies and keep a sharp eye on data collection, since consumers value it so highly.

That would suggest that compliance officers should draft strong privacy policies and keep a sharp eye on data collection, since consumers value it so highly. Here's the thing, though: evidence taken from court cases suggests that belief might be misguided.

At least, that's the implication of another bit of research published in 2013, "Empirical Analysis of Data Breach Litigation." The authors (led by Sasha Romanosky, professor of IT systems and public policy at Carnegie Mellon University) studied more than 1,700 reported data breaches in the 2000s, which led to 230 lawsuits in federal court. The paper reached some conclusions that would warm the legal department's heart:

» Most data breaches never result in litigation;

» Most breaches that do result in litigation are settled because the plaintiffs can't demonstrate actual harm;

» The odds of a company being sued are 3.5 times higher when individuals suffer financial harm;

» The odds of a company being sued are 6 times lower when the company offers free credit monitoring.

Put the conclusions of these two papers together, and a bigger picture starts to emerge. First, when a data breach occurs, all those fulminations from consumer advocates and plaintiff lawyers might be beside the point, because consumers don't suffer much actual harm.

After all, for most victims of a breach, the risk isn't that you'll check your bank account one day and find no money; it's that you apply for a mortgage one day and find someone else already ruined your credit by opening false accounts under your name. With proper credit monitoring that threat is reduced, and consumers aren't liable for more than $50 in bogus credit card purchases anyway. From their perspective, then, why care? The false purchase is someone else's problem.

Of course, from the compliance officer's perspective, the false purchase is still your problem, since the company still has to pay the cost for that stolen product or reimburse a customer for stolen money. But the Romanosky paper, at least, shows that when thieves steal customer data, the steps to placate customers can often be straightforward. Far more important is spending your time working with the IT and internal audit departments on proper IT security and access controls. (Another finding of the Romanosky paper: consumers are less likely to sue if their data was indeed stolen by hackers who somehow pierce your IT security; and much more likely to sue if their data is lost by employee ineptitude like losing a laptop on the subway.)

More problematic for compliance officers is the NERA study, and its conclusion that consumers dislike the idea of companies collecting and sharing data about their behavior. That's a tough question of business ethics, because plenty of companies now thrive on collecting and sharing information about their customers—but consumers value privacy as a prize unto itself, even if the real harm of losing privacy might be small, as the Romanosky study suggests.

Still, your privacy policy *will* need to answer that ethical question sooner or later—and if you don't give an answer that demonstrates restraint and transparency, expect the Federal Trade Commission or plaintiff lawyers to provide an answer for you.

Rules Change to Ease Export Controls in the Cloud

by Jaclyn Jaeger
July 7th, 2015

Good news: New amendments to U.S. export control regulations are on the horizon that could ease licensing requirements when storing or transmitting technical data or software in the cloud—although, naturally, the regulations come with a catch.

In June the State Department's Directorate of Defense Trade Controls and the Department of Commerce's Bureau of Industry and Security published proposed rules amending yet more acronyms, the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Overall, the proposed changes are designed to "facilitate compliance with export controls, update the controls, and reduce unnecessary regulatory burdens on U.S. exporters," the BIS rule stated.

U.S. export control laws apply not only to the shipment of physical products out of the United States; they apply to the technology and software necessary for the development, production, or use of those products, too. That means every time controlled technology or software is transmitted through the cloud outside the United States to a foreign country, the government deems it an export, potentially subjecting companies to violations of U.S. export laws.

"One of the biggest challenges for U.S. companies is determining where the servers are located that will be storing their data," says Cheryl Palmeri, with law firm Bass Berry & Sims. That's a big problem, because if servers are located in countries subject to U.S. export restrictions, the cloud users themselves could be considered in violation of U.S. export rules.

In some cases, "defense manufacturers have tried to negotiate outsourcing arrangements for storage of data, and because servers were located in countries outside the United States, they simply had to cancel the deals," says Christopher Wall, senior international trade partner with law firm Pillsbury.

> "If you're going to use encryption outside the [NIST] standard, it better work is what they're saying."
>
> John Eustice, Miller & Chevalier

The DDTC and BIS proposed rules would go a long way to ease those compliance burdens by changing the definition of "export" to allow companies to store information in the cloud in servers located in foreign countries, as long as the technical data or software is encrypted to prevent access by foreign persons. If approved in their current form, the new rules "could make export control compliance easier," Palmeri says.

Comments on the proposals are due by Aug. 3.

"For defense articles, that makes a huge difference," Wall says. "It means that large defense companies like Lockheed Martin and Boeing that have technical data subject to ITAR controls can now use cloud storage services outside the United States. That's a big change."

Both the DDTC and BIS proposed rules spell out similar circumstances where "sending, taking, or storing" technical data or software would not be considered an export. Specifically, technical data under ITAR, technology under EAR, and software must be unclassified and secured using end-to-end encryption. As explained by the BIS proposed rules, encrypting data "involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient."

In that respect, the proposed rules don't eliminate compliance obligations altogether. Instead, changing the definition of "export" in the context of cloud computing would shift the compliance emphasis from identifying the location of servers to ensuring that appropriate encryption safeguards are in place, Wall says.

One important difference between the DDTC and BIS proposed rules is that DDTC strictly requires that encryption standards be certified by the National Institute for Standards and Technology in compliance with federal cryptographic standards. The DDTC further would require that encryption be "supplemented by software implementation, cryptographic key management, and other procedures and controls" in accordance with guidance provided by current NIST publications.

In contrast, the BIS proposed rule states that "alternative approaches are allowable provided that they work. In such cases, the exporter is responsible for ensuring that they work."

"It's basically saying, 'Buyer beware'," says John Eustice, a member with law firm Miller & Chevalier. "If you're going to use encryption outside the [NIST] standard, it better work is what they're saying."

Another way that companies can violate U.S. export laws under the proposed rules is if a foreign person—whether a foreign employee here in the United States, or a foreign person abroad—gains access to controlled data in the cloud. So it's important to "screen whomever you're doing business with to ensure they're not located in a prohibited country and are not a prohibited party," Palmeri says.

Specifically, the DDTC and BIS proposed rules state that sending or releasing encrypted data (cryptographic keys, passwords, network access codes, and the like) would trigger an export control violation. What the rules don't discuss is standards for password security, "which is kind of like closing the back door but leaving the front door wide open," Eustice says—since most big hacks result from password breaches.

It's also important that companies pay attention to the storage restrictions laid out in the proposed rules, says Alexandra López-Casero, a partner with law firm Nixon Peabody. For example, the proposed rules prohibit companies from storing controlled technical data in certain restricted countries: China, Iran, the Russian Federation, for example.

That means cloud users need to get that certification from the cloud service provider. "Having seen some of these contracts, some of them are ridiculously simplified, and they need to cover a little more area," Eustice says.

"It's important to know not only where your data will be stored, but also where it will transit," Palmeri says. "We advise companies to ask cloud providers those questions and to include provisions in their contracts prohibiting their data from being exported to or stored in specific countries subject to U.S. export controls or sanctions laws," she says.

Welcome Guidance

Until the proposed rules, little guidance has been issued for cloud computing and export control items. In 2009 and 2011, BIS issued two advisory opinions in which it "basically took the position that compliance responsibility rested with the cloud user," Wall says. BIS essentially concluded that cloud providers offer a service, and therefore aren't "exporters" of controlled technical data.

Enforcement action on this front has also been non-existent, which is "not necessarily surprising, given that a lot of that stuff happens behind closed doors through internal investigations," Eustice says.

In cases where companies have self-disclosed potential export violations in the course of using cloud computing services, "the agency declined to impose any penalties," Palmeri says. Why? Probably because agencies understand that this is a new area where export control regulations don't quite fit, she says.

In March 2014, for example, software-development company Zendesk disclosed in its initial public offering with the Securities and Exchange Commission that it may have violated U.S. export control and sanctions laws, resulting from its acquisition of Singapore-based Zopim, a live-chat software solution provider. Prior to the acquisition, Zopim provided services from servers based in the United States to a number of persons and organizations located in Iran, a country subject to U.S. economic sanctions.

"Zopim also made available for download from the United States certain encryption-functionality software without first having obtained U.S. government authorization to export such software," Zendesk stated. "In these instances, Zopim may have acted in violation of U.S. export controls and sanctions laws."

As a condition of the acquisition, Zendesk said that Zopim ended the subscriptions to customers in Iran, screened its customers against a U.S. list of prohibited persons, implemented measures designed to prevent future unauthorized access to the service, and obtained U.S. government permission to export its software.

"It's important for companies to look at these proposed rules and see what the effect will have been to them and provide comment," Palmeri says. "The agencies right now really are looking for feedback from industry on what this will mean if these rules are implemented."

COMPLIANCE WEEK

The Role of Compliance in Adopting Data Privacy Controls

by Joe Mont

October 21st, 2014

Around the world, governments are responding to the massive trove of personal data companies and healthcare entities are amassing and a rash of data-security breaches with new, strict guidelines, regulations, and laws. In response, privacy and compliance programs are increasingly at an intersection.

Unfortunately, working together is often easier said than done, and the regulatory focus on data raises an abundance of questions. Should compliance oversee privacy, or must they be independent? What defines a healthy working relationship among those involved, including compliance, IT, marketing, and the board? What is the prescription when these separate interests are at loggerheads? A panel of privacy experts addressed these questions, and others, during a session at the Compliance Week Europe Conference in Brussels.

Build Bridges

A key to bringing compliance and privacy together lies in diplomacy, Jennifer Aikins-Appiah, regulatory compliance officer for CPA Management Services, said. When implementing a privacy program, even one with top-level sign off or executive sponsorship, departmental silos need to be broken down.

"There is no point implementing something that no one is going to buy into," she said. "Ultimately these are going to be the people who ensure compliance among their staff. They are going to be your gatekeepers."

> "I don't mean put on your boxing gloves and wage world war within your organization; what I mean is to have open conversations."
>
> Jennifer Aikins-Appiah, Regulatory Compliance Officer, CPA Management Services

Reaching out to middle management and IT and privacy corners of an organization, rather than issuing marching orders, is far more effective in getting buy-in and much-needed help, Aikins-Appiah said. However, compliance officers shouldn't fear standing their ground when the need arises. "Sometimes you do have to be a little confrontational," Aikins-Appiah said. "I don't mean put on your boxing gloves and wage world war within your organization; what I mean is to have open conversations. Some of the concerns may actually be justified and valid because the people you are talking to have more experience with the departments you are trying to reach and the things you are trying to implement. Their advice will help your policy go much further."

After a privacy program is implemented, a compliance officer should maintain his or her charm offensive," Aikins-Appiah said. "Don't become invisible," she said. "You have a privacy-by-design program you want everyone to abide by, but then go and sit at your desk all day where no one can see you? Put yourself out there. Try to engage not just with the managers but all levels of staff." This outreach will help give the CCO a better view of what is happening in these various entities. "You want to be on the forefront of any potential risks around data breaches," she added."You need to be on the ball."

Watch the Headlines

Being on the ball also requires knowing what is happening around the world, not just within company walls, Aikins-Appiah said. When Canada passed its new anti-spam law it had implications on marketing efforts, and those issues had to be dealt with immediately. Enforcement matters must also be keenly watched as they give a sense of governmental priorities and help set company risk weights.

Other developing trends include E.U.-wide privacy rules that, although delayed, could go into effect by 2017; the continuing U.S. crackdown on healthcare data breaches; and the growing concern over Big Data.

Multiple Hats, or One?

Should privacy and compliance be melded together? Uwe Fiedler, global privacy officer for Parexcel International, a pharmaceutical research company, sees value in keeping the various efforts within each function separate.

"It is helpful to have separation," he said, explaining that the role of both compliance and privacy officers is to report risks to the board and leave the matter in their hands. To ensure that the board takes matters such as privacy and breach notifications seriously, he suggests a firm recitation of all the executives and board members who have either lost their job or gone to jail for their negligence.

"One of the issues is of size and scale," countered Jose Tabuena, chief compliance officer for Next Health (and a Compliance Week columnist). "At smaller, mid-size companies it is probably too much to have a chief in every area—chief information security officer, chief information governance officer, chief anti-trust officer. All of these to typically fall under the risk domain of compliance, which is the overarching framework. In most of my experience the chief compliance officer is also the chief privacy officer." At his company, a healthcare start-up, he serves as the compliance officer and has a privacy specialist who reports to him. That specialist and has more day-to-day responsibility for privacy issues.

Tabuena did concede, however, that in some industries the "privacy risk might be so large that you start having to put more resources in that area."

What's on the Horizon?

The need for compliance, privacy, and IT to work cooperatively will only become more pronounced in the months ahead.

At the conference, Sophie Nerbonne, deputy director for legal affairs and director of compliance at France's Commission Nationale de l'Informatique et des Libertés, discussed the state of privacy protection measures in France and throughout Europe. CNIL is an independent regulatory body that oversees the application of privacy law to the collection, storage, and use of personal data. It is comprised of 17 members from various government entities in France, including four from its parliament.

> "A lot of work has been done and there are just a few points to clarify. "
>
> Sophie Nerbonne, Deputy Director, Legal Affairs and Director, Compliance, France's Commission Nationale de l'Informatique et des Libertés

In January, CNIL issued a ruling that Google's privacy policy did not comply with French data protection laws and issued a fine of €150,000. More recently, CNIL was behind a September "cookie sweep," a series of not-so-surprise company audits to assess compliance with French and European Union rules requiring websites to obtain user consent before installing cookies, those tiny bits of data that get popped onto your hard drive every time you visit certain websites. Users must also have the ability to know how cookies are used and to opt-out of the data collection.

Nerbonne updated the audience on the status of long- delayed EU-wide personal data protection legislation. Negotiations will soon restart on a new law that would consolidate the data protection regulations of individual EU member nations. An ongoing point of contention among business leaders is that the new law may demand breach notifications within 24 hours of an infiltration, without any safe harbor for data encryption.

Other measures likely to be included in the legislation are the right to portability of personal information, the "right to be forgotten," requiring a project- and product-based Privacy Impact Assessment; and fines €100 million or 5 percent of global turnover for companies that transmits personal data outside the EU without a customer's permission. "A lot of work has been done and there are just a few points to clarify," Nerbonne said. "We are still hoping that by the end of the first part of next year it will be done and then it will take two years to put the new regulation into application."

"The challenge with the U.S. Health Insurance Portability and Accountability Act and other standards are that, on one hand, they are flexible and agnostic in terms of technology," Tabuena said. "On the downside: They are flexible. They don't really give you a lot of specifics on what it means to be secure and what is a reasonable control. That is where I am going to need to rely on the IT and information security experts to help me out."

Their assistance, and the help of the legal department, can help map out what threats exist and the priority status that should be placed on them. "It's a lot of work, but you have to start somewhere," Tabuena said. "You have to put together a country-by-country, state-by-state matrix of all the breach rules, including how they define sensitive information."

Three Ideas for Compliance, Audit, and Cyber-Security

by Matt Kelly

February 8th, 2015

Nobody can get enough guidance about cyber-security these days, and the New England Chief Audit Executives group is no exception. I attended the group's winter meeting here in Boston, and that's all we talked about for two solid hours. These folks had good ideas galore about managing cyber-security risk, so let me recap the most important ones here.

First, worry more about the process of how information is governed at your business than about the tools you use to protect it. The discussion started with a panel of audit and IT executives, and every one of them agreed on this point. Tools address one specific risk, and they may do that quite well—but they may also be useless for every other risk. And if your process for governing information is sloppy overall, those other risks will hit you eventually. The tools you have won't do you much good then.

I always favor analogies from the real world, so try this one: at some point in life you might suffer a heart attack. You can go through life equipped with tools to reduce that risk, such as a defibrillator, and it will indeed help when the time comes. Or you can *improve your process of being healthy*: eating right and exercising. Neither one of those procedures will assure that you never have a heart attack—but they will help you immensely in staying alive should a heart attack come to pass.

Good tools without good process is the equivalent of carrying around a defibrillator while you overdose on salty foods and sit on the couch all day. Does that sound like a good strategy for preventing heart attacks to you?

Second, define the roles for managing cyber-security risk at your business. Nobody at the CAE group specifically mentioned the Three Lines of Defense model, but that's my default for any conversation about who oversees what part of a risk. In that case, the internal auditors have things a bit easy: you're in the third line as usual, testing the security procedures and controls like you would any other.

The first and second lines of defense get more complicated. Clearly IT (or the IT security function, if you have a separate one) belongs in the second line. Compliance does too. But each one supports the business units bravely holding down the first line of defense in different ways. My first point above, to worry more about process than tools, still holds true—but you do need both tools and process to have effective cyber-security: IT supporting the tools to fight cyber-security risks, compliance supporting the processes.

> I like to think of effective cyber-security defense as this: for business units to follow effective processes there in the first line, compliance needs to do its job in the second line defining what those processes are.

I like to think of effective cyber-security defense as this: for business units to follow effective processes there in the first line, compliance needs to do its job in the second line defining what those processes are. They might be policies to have third parties certify their data security, or procedures for swift disclosure of a data breach. But the business units can't follow a good process unless compliance does its job spelling out the policies and procedures that govern that process.

The third point I heard, and perhaps the most heartening one, was that Corporate America has faced a mess of poor controls and poor understanding of risk before—and we solved the problem. We've been here before with Sarbanes-Oxley compliance.

Numerous times I heard speakers worry about weak processes and then breezily add, "unless it's a SOX process, because our SOX processes are generally strong," or "If it's a SOX-related control usually we're confident it works."

Study those parallels between SOX compliance and cyber-security, because they are deep and vital. A huge amount of cyber-security risk hinges on access: ensuring that only authorized users get access to certain types of data. That is the same worry compliance and internal auditors have about access control to financial information—and you've been testing your access controls for financial data for the better part of a decade. Drop the word 'financial' from my last sentence, and you have your marching orders for cyber-security risk. I'm not saying that goal is easy to achieve, but that's the goal.

You can even make an intellectual leap from SOX compliance back to the importance of a strong process. When you read through the 17 guiding principles of the updated COSO framework—the framework we're all using for SOX compliance—those principles are all about strengthening your process. Everyone might be using the framework right now for internal control over financial reporting, but COSO intended the framework to be a roadmap for internal control over other risks too, cyber-security included.

So as scary as cyber-security might be right now, it can be conquered. If the compliance and audit community tamed Sarbanes-Oxley, you're in prime fighting shape for this threat too.