DataMotion™

Better Watch Your Tail...

You Might Be Violating Data Security Laws You Haven't Even Heard of Yet!

As laws surrounding data security evolve and grow, they're extending to thousands of additional businesses that may not realize they're subject to new regulations. Under these laws, if your business interacts with companies that collect, store or otherwise process individuals' personal information—whether it's credit card numbers or medical lab work—you may be required to exhibit the same level of care with regards to the security of that information as the companies that collect it.

In fact, you may have already violated one or more of these laws unknowingly. It's no longer clear-cut which laws pertain to which kind of organization. For instance, you may need to be *PCI*- or *HIPAA*-compliant, even if you don't process credit cards or provide medical care. Compliance violations can put you, your customers, and your business at serious risk. And a primary point of risk exposure is email—but there is an effective way to mitigate that risk.

The Long Tail of Regulatory Compliance

Several laws related to data may apply to your business. One is the **California Breach Notification Law**, which defines:

(a) the conditions under which a person's "unencrypted personal information … was acquired, or reasonably believed to have been acquired, by an unauthorized person," and

(b) the actions that must be taken if a security breach occurs.

The law was amended effective January 1, 2014 to expand the definition of "personal information." It now includes first name or initial in combination with a last name and any of the following: Social Security number, driver's license number, credit card number, username/password for a website, and several additional items. If a data breach occurs, the sender must immediately issue a breach notification—informing the recipient, the state Attorney General's Office and the general public.

The California Breach Notification Law applies to any company that conducts business in California. As the most populous state, it's likely that this law applies to you if your business has a national customer base. Even if you don't do business in California, its legislation often eventually influences other state and federal laws, so similar laws may soon apply to your state.

Another important law is **HIPAA (Health Insurance Portability and Accountability Act)**, which was enacted in 1996 and has expanded its reach substantially since then. The **HITECH Act** of 2009 updated HIPAA rules effective September 2013, so that they now apply not just to medical providers, but to the entire ecosystem of vendors supporting them.

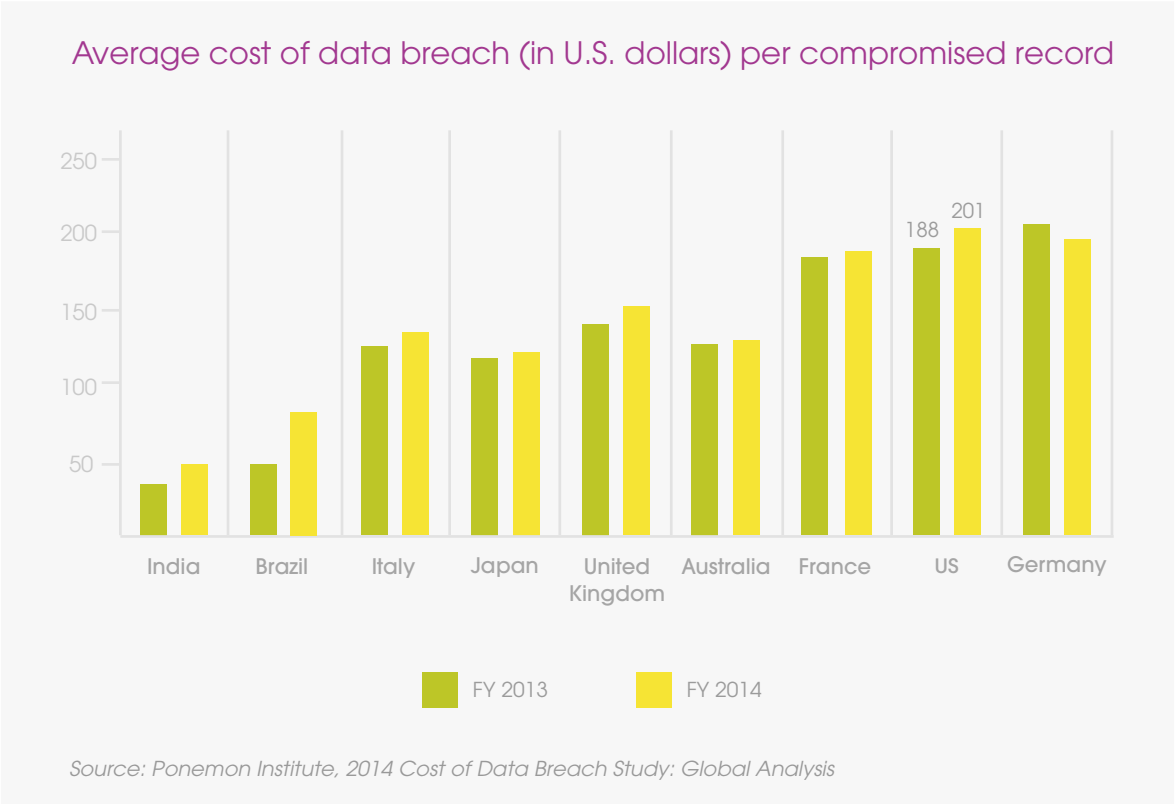
Anyone exposed to patient information—be they labs, third-party billing companies, even janitorial service companies—could qualify as "Business Associates" under HITECH and therefore be subject to the same standard of privacy and security as the medical provider they service. We call this the long tail of liability, because it affects everyone down the chain of customer interactions.

The **PCI (Payment Card Industry) Data Security Standard**, which regulates the security of credit card information stored, processed or transmitted by merchants and associated vendors, also exhibits this long tail. Though technically not a law, there are laws at both the state and federal level that effectively force PCI compliance. Therefore, any business that uses credit card information should have PCI on its radar. This could include organizations ranging from financial institutions to e-commerce software vendors to online data hosting companies.

A fourth relevant law is the **Gramm–Leach–Bliley Act (GLBA)**. Enacted in 1999, this law requires financial institutions to publish and follow a privacy policy, which they supply to their customers upon first purchase/use of service and annually thereafter (or whenever it changes). You've probably seen these notices from your credit card providers, or when you sign up on certain websites. The challenge here is that your business may qualify as a financial institution without even knowing it. Any business that provides any kind of financial service—which includes insurance agents and companies that provide investment advice—is subject to this law.

Ramifications of Non-Compliance

Major data breaches are embarrassing—and expensive. A 2014 study from the Ponemon Institute showed that in the U.S. the average cost of a security breach was $201 per compromised record:[1]



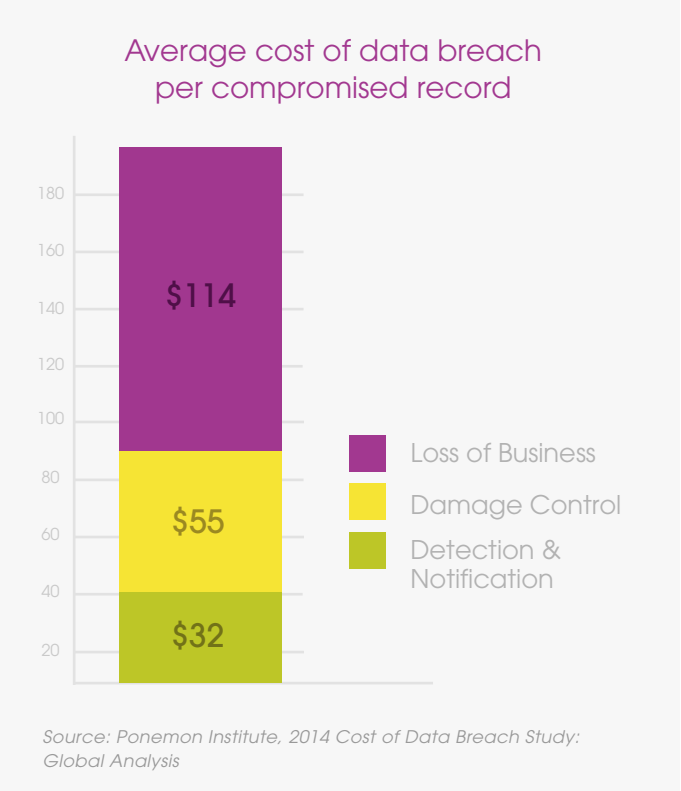
Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis

[1] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*

There were three components to this cost:

- The cost of identifying the breach and applying all the legally required notifications ($32 per record).
- "Damage control," which includes help desk activities, investigation, remediation, fines and legal costs ($55 per record).
- Loss of business, which was over $114 per compromised record. For some businesses, of course, the lifetime value of a single customer greatly exceeds that.

When customers' data is compromised, it exposes them to the risk of identity theft, which costs the average victim $500 and 30 hours to resolve.[2] If your company's inadequate safety measures are responsible for the breach, those customers will associate all of that expense and frustration with you. When the time comes for them to decide whether to retain your services, it will be understandable if they hesitate.



Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis

The inability to acquire new customers is another significant impact of a data breach. Major data breaches are big news, and just as your old customers may cancel their contract with you at the first chance they get, new customers will think long and hard before coming on board. Most companies rebound eventually, but in the short term, a data breach can stall sales cycles, and the stigma associated with it is yet another long tail in the memories of prospective customers.

Even if you never experience a breach, companies (and individuals) are increasingly reluctant to do business with organizations that aren't compliant with data security laws. Media attention about breaches at major corporations and individuals' experience with identify theft have led people to be more sensitive about data security. As a result, many people only want to do business with companies they believe are taking the extra steps necessary to ensure compliance.

Put differently, a robust compliance initiative can make your company more attractive to prospective customers and partners. And the cost of compliance will be negligible compared to the $201/record average price tag of a security breach.

Finally, it's important to keep in mind that these data security requirements are the law, which means that you could be subject to major fines for failure to comply.

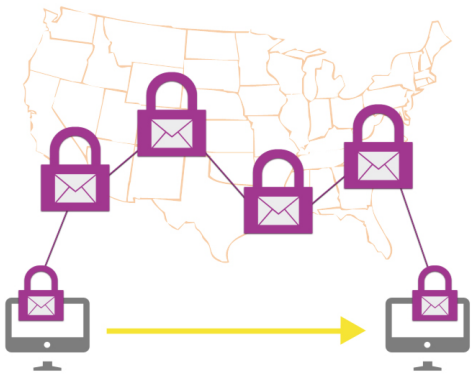
Email: A Big Threat

There are many different threats to data security and remaining in compliance, and one of these is email. On average, each corporate employee averages 156 minutes of email use,[3] and sends/receives 115 messages per day.[4] Since email is so ubiquitous, many people use it to send sensitive information like passwords or credit card data unwittingly. Sometimes people "know" they shouldn't send this information over email, but often they are simply unaware of the associated security risk and liability.

[2] TransUnion, Identity Theft Facts

[3] McKinsey Global Institute, "The social Economy: Unlocking value and Productivity Through Social Technologies," 2012

[4] The Radicatti Group, Inc., "Email Statistics Report," 2013 - 2017



The primary reason standard email is not secure is a reliance on the public Internet to get it to its destination. Messages get routed through a number of different locations on their way from one server to another. Although the connection between your computer and your email server may be secure, the connection between your email server and that of your recipient usually isn't. If someone is committed to accessing your information, they will do it during the transit period. Even after the recipient has opened and deleted the vulnerable message, it's still out there in the ether.

In essence, using standard email to send sensitive data is like sending private information on the back of a postcard. It's easy to intercept and read. Do you really want to take that risk?

Encryption: The Easiest Path to Protecting Email

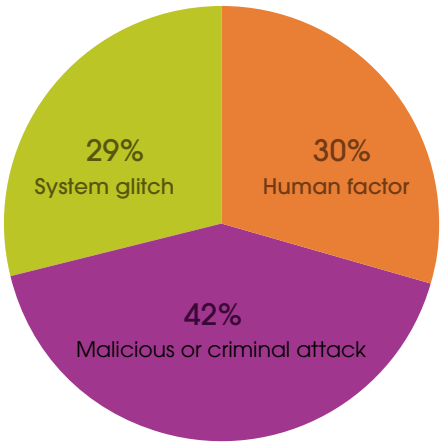
Complying with the various laws that affect data security is a major undertaking. It involves a mix of technical, procedural and administrative tasks—and many businesses are unsure where to start. But the ubiquity of email suggests that it is a good thing to tackle early on.

By protecting data transfers over email, companies take a step toward achieving compliance and avoid costly data breaches that damage customer and business partner relationships. If you do have a breach but the data is encrypted, in some states the encryption exempts you from most concerns. This means the costs of the breach will be far less than if you are operating without a compliance program in place.

Email encryption software and services integrate with your standard email clients and systems to encrypt messages containing sensitive information and password-protect them so that only the recipient can open them. Compared to the $201/record price tag of a security breach, the annual per-record cost of data encryption software would be measured in pennies.

Some important things to look for in email encryption software include:

- Seamless integration with your existing systems so you don't need to implement any new clunky processes or protocols.
- Ease of sending large files containing sensitive information like financial statements, healthcare claims, and legal documents.
- Sender notification when the email has been received, so the sender is assured that the information was delivered securely.
- Continuous monitoring of email for sensitive content and automatic encryption, since 30 percent of security breaches are a result of some human factor.[5]



Distribution of root cause of data breach

Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis

[5] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*

- Mobile platform support. Statistics on mobile email use vary drastically (from 15 percent up to 65 percent), but one way or another, more people than ever need to access and send their data from mobile devices. Data encryption software needs to integrate seamlessly with those devices, too.

Take Action Before It's Too Late

The potential consequences of not complying with data security regulations are far-reaching and varied—from government-issued fines to enormous sums spent on damage control. The longer you wait to protect sensitive data and move closer to regulatory compliance, the greater your chance of being affected by a fine or a data breach. The good news is that solutions are available today—so it's up to you to make data security a priority before it's too late.

DataMotion, Inc. provides secure data delivery solutions such as encrypted email. By using DataMotion, businesses can safely and easily exchange email, files, and other information with partners and customers in the cloud. Our easy-to-use solutions for encrypted email, file transfer, forms processing, customer contact and the Direct Project leverage a core, secure platform for unified data delivery. All our solutions apply compliance-grade encryption to your emails, attachments, and files, including those sent from mobile devices, allowing them to travel across the Internet untouched and safe.

DataMotion™