The impact of global privacy laws on cyber risk mitigation
The impact of global privacy laws on cyber risk mitigation

Introduction

A data security breach that compromised the personal information of about 100 million customers of a giant U.S. retailer in late 2013 has cost the company about $164 million, including the cost of updating its data security technology. The data breach also factored into the company’s decision to replace its chief executive officer and chief information officer a few months after the incident.¹

In one of a series of recent major cyber thefts of personal information in South Korea, the credit card details and other personal data of 20 million individuals were stolen in early 2014 by a hacker at a computer contractor retained by a leading credit bureau in the country. As part of their investigation, South Korean authorities launched inquiries into the data security measures at three major South Korean credit card companies after evidence suggested the hacker accessed the bureau through one of those companies’ systems.²

Hackers are being blamed for stealing yet-undetermined sums of digital currency in early 2014 from a major Tokyo-based bitcoin exchange. The theft forced the exchange to shut down, seriously threatening its future and triggering lawsuits by its customers. Estimates of the value of the cyber theft, which affects the exchange’s customers worldwide, range from millions of dollars to more than $500 million.³⁴

The June 2014 data security breach that jeopardized the credit and debit card information of thousands of customers of a U.S. restaurant chain with more than 200 locations nationwide has drawn the attention of the U.S. Secret Service.⁵⁶ More than a month after the incident, which the company’s chief executive officer says was executed by a highly sophisticated criminal operation, the chain’s restaurants were still using manual card-imprinting systems.

Those examples of computer security breaches are not exceptions but instead exemplify the cyber risk that every organization with a computer system and an Internet connection faces, no matter where they operate in the world, according to research and experts in the field. Particularly telling of the worldwide cyber risk exposure is the abundant number of known breaches, even though data privacy laws in many countries outside of the United States currently do not require the companies they regulate to publicly disclose those events.

Those laws, however, likely will stiffen in coming years. Already, the European Union is close to implementing much more stringent data privacy regulation that would impose greater disclosure and customer-notification requirements on companies that suffer a breach. Several countries in Asia and Latin America already have passed such legislation. Tougher regulation only will exacerbate the continually growing financial impact of cyber attacks.

As the potential costs of security breaches grow and risk management experts begin convincing senior company management worldwide that all organizations are vulnerable and will suffer some kind of breach eventually, enterprises across the globe likely will consider cyber risk insurance as a risk-financing option. For multinational companies, however, covering operations in another country under a non-admitted global master program rather than a locally admitted insurance policy could lead to a multitude of complications in the event of a loss.

2. Credit card details on 20 million South Koreans stolen. Jan. 20, 2014. BBC.
The numbers

Even though personal data privacy laws in many countries worldwide do not require companies to notify customers when their personal information has been stolen or compromised, many cyber security researchers and consultants have mined enough information about these events to expose the magnitude of cyber risk.

The findings of PricewaterhouseCoopers’ survey of 9,681 corporate executives from companies of all sizes in 115 countries underscore that the number of known data breaches reflects only a fraction of the security incidents organizations face. PwC questioned survey respondents in February 2013 about all of their security incidents, not just breaches, over the previous 12 months. Those incidents include “any adverse incident that threatens some aspect of computer security.” Survey respondents reported that their organizations each faced 3,791 security incidents on average, or more than 10 incidents every day. That’s a nearly 27 percent increase from the 2,989 incidents that respondents reported in the year-earlier survey and a 48 percent increase from the 2,562 incidents reported two years earlier. But nearly one-fifth of the respondents — 18 percent — could not answer the question in the latest survey, double the percentage from two years earlier.

Yet, between 76 percent and 84 percent of the surveyed C-suite executives reported they were confident in their security systems. Chief executive officers were the most certain, while chief financial officers were the least. Overall, 74 percent of survey respondents were confident in their security systems.

Menace behind the numbers

Who is after all of that personal data? A major source of the problem is professional criminals, who clone the payment card information they steal onto counterfeit cards that are then sold.

But highly motivated parties with other agendas also are responsible for security breaches. Some states as well as industry competitors engage in cyber espionage in bids to steal intellectual property. Other times, those same actors commit cyber sabotage, disrupting or damaging computer networks or manipulating them in a way that causes physical damage at a separate physical site those systems are instrumental in controlling. In addition, parties with political agendas — or hacktivists — breach the systems of organizations they have idealistic conflicts with, intending to disrupt their operations and damage their reputation.

Several factors exacerbate organizations’ already significant cyber risk. A critical factor is that many organizations see plenty of opportunities to trim expenses by cutting back on technology. But those measures typically increase the risk of cyber attacks.

For example, the voice over Internet protocol, or VOIP, telephone service is less secure than landline telephony. Similarly, Cloud computing is more cost-efficient but considered less secure by many risk management professionals. Allowing employees to use their personal IT devices — including smartphones, tablets and laptops — at work is both a cost-saving and a morale-boosting measure, but it can expose the organization to much greater cyber risk. In addition, the Internet of Things — the concept of connecting everyday objects other than computers, smartphones and entertainment devices such as televisions and DVD players to the Internet — also dramatically increases organizations’ vulnerability to security breaches. With Internet-linked fax machines and security cameras, IoT already has created cyber risk for many organizations.


9. Ibid.

The criminals who are attempting to breach organizations’ security also have become far more sophisticated in how they mount their attacks by designing malware specifically for a particular target, which can significantly boost the odds they will breach the organization’s security sooner rather than later. Before launching an attack, these hackers will study the organization for a security weakness they can exploit to jump into its system undetected.

That opening, for example, could be a vice president who plays fantasy football and who might not think twice about opening an email — sent through the executive’s company account — from a seemingly legitimate sports website purportedly providing some important game insight. When the executive opens the email, which would contain legitimate information to avoid arousing suspicions, the malware imbedded in the message quietly enters the company’s system.11

Hackers recently found a different inroad to an oil company’s system they previously had been unable to breach. They infected the online menu of a Chinese restaurant that is popular with company employees. When company employees opened the menu online, it delivered the hackers’ malware to the company’s system.12

Making hackers’ jobs significantly easier are online security flaws that are even greater than any organization’s own inadequate measures designed to safeguard customers’ personal information. Two such flaws were revealed in early 2014 alone.

One is the Heartbleed security flaw in the open-source encryption technology OpenSSL. Around two-thirds of Web servers around the world use the technology to protect all kinds of personal information, including financial information, collected by HTTPS websites. Heartbleed resulted from a coding error in the encryption technology in March 2012. So for two years, Heartbleed allowed hackers to both steal personal data from servers and create bogus duplicate websites to collect personal data directly without anyone even knowing that risk existed. To fix the problem, the affected websites as well as individuals have to take various measures.13

Just weeks after the Heartbleed security flaw was revealed, Microsoft announced a major security flaw with versions 6 through 11 of its Internet Explorer browser. The flaw gave hackers using network computers the same level of access as the legitimate user, jeopardizing the personal information of millions of IE users. Cybersecurity software maker FireEye reported that the flaw allowed a group of hackers to attack U.S. financial institutions and defense firms. Microsoft issued a patch to fix the flaw five days after revealing it.14 15

The Heartbleed and Internet Explorer incidents are hardly isolated examples of security flaws outside of an organization’s control. For example, users of Apple’s iPad and Web browsers Firefox and Safari also have been victimized by security flaws and breaches.16

---

11. Ibid.
13. The ‘Heartbleed’ security flaw that affects most of the Internet. Heather Kelly. April 9, 2014. CNN.
Game changer

When security breaches occur, the data privacy laws in many countries around the world do not require the victimized organizations to notify customers or clients that their personal information has been stolen or compromised, although data privacy regulators might have to be informed. In comparison, the laws in 47 U.S. states, the District of Columbia and several U.S. territories mandate that breached companies notify their customers and clients.

But a U.S.-like regulation model that imposes notification responsibilities on breached organizations is heading to Europe, and that could compel other countries to modify their data privacy laws similarly.

Currently in Europe, regulations covering data breaches are inconsistent, as is their enforcement. For example, in Italy, organizations — except providers of publicly available electronic communication services — have no obligation to notify customers or clients when their personal information has been compromised. In the United Kingdom, there is no notification obligation outside of the Telecoms Act, but the country’s data privacy regulator requests that it be notified if a breach affects a large number of individuals. France has a layered notification requirement that begins with the country’s data privacy regulator and could extend, at the regulator’s discretion — to the individual affected by a data breach. Germany requires organizations to notify the affected individuals if the breach likely would severely harm their rights and interests.

While the United Kingdom and Spain rank first and second, respectively, in both the highest number of data privacy complaints and the highest regulatory fines on average, organizations face the greatest risk of regulatory fines in Portugal and Romania. The maximum allowable fines also vary widely among E.U. countries, ranging from nearly 607,000 Euros in the United Kingdom, 150,000 Euros in France and 20,000 Euros in Portugal.

The European Commission’s data privacy protection reform proposal would harmonize and largely stiffen the various privacy rules among the 28 E.U. member states and three Economic Area states that are not E.U. members. Among other provisions, the reforms would require organizations to notify regulators and possibly customers and clients with the details of a data breach without delay. The reforms also would establish a fine of up to 2 percent of a company’s worldwide annual revenue if local regulators determine the company had violated the directive’s data protection provisions.

In addition, organizations that are not based in Europe but operate there or intend to would have to fully comply with the reforms — including the penalty provisions.

The European Parliament and individual E.U. member states still must act on the proposed directive, so many observers do not expect the proposal to take effect until late 2015 or sometime in 2016.

If the data breach notification reform survives, as expected, many other countries around the world can be expected to adopt a similar measure to maintain their reputations as attractive trade partners with the European Union. Already, lawmakers in Brazil — one of the countries in the BRICS bloc of important emerging markets — are considering data privacy reforms based on the E.U. proposal. In addition, Canada, Australia and New Zealand are moving in this direction.
In the meantime, companies with operations in countries — particularly in Europe and Asia — where data privacy laws that do not include breach notification provisions still face some steep costs besides regulatory fines under those regulations. The data privacy laws in some of those countries require the breached organizations to erase any wrongful use of an individual’s identity as a result of the breach and remedy any damages — a process that can become complex and expensive.28

Risk-financing considerations

A data breach can result in numerous expenses: breach forensics, updated technology and software, data restoration, business interruption, data breach notifications, remedies for wrongful use of data, regulatory fines, litigation defense and settlements or court awards.

A breach also could trigger a lawsuit against an organization’s directors and officers, if shareholders believe the entity had particularly lax data security or had inadequate cyber-risk financing in place to cover the costs stemming from a data breach. D&O insurance typically would not cover those costs, including any errors and omissions liability claims filed by clients of a service organization.29

A compromised organization likely will incur at least some of those expenses and possibly all of them, depending on where in the world their customers and clients reside. As more countries toughen their data privacy laws, the potential data breach costs for a hacked organization will only increase.

As a result, more organizations around the world — as a growing number of companies already have — likely will consider financing their cyber risk, which could amount to millions of dollars in expenses for a single breach. For example, after a breach, a middle-market company with $1 billion of annual gross revenues globally could face a $2 million fine under the E.U.’s proposed data privacy reforms. That loss would not include any of the other potential costs that could arise from a breach.

Risk management at a multinational organization might consider insuring its global cyber risk under a single insurance policy offering worldwide coverage for the entire entity. But that risk-financing strategy — compared to purchasing a true international program with a master policy and separate, locally admitted coverage within each country where the organization has cyber risk — could create indemnification and tax problems for an organization that suffers a covered loss.

Many countries around the world do not allow non-admitted insurance. According to Axco Insurance Services, Ltd., only a couple dozen countries worldwide — mostly in Europe — allow non-admitted insurance. But some legal experts say there are even fewer.

In still more countries, there are conflicting legal interpretations of the permissibility of non-admitted insurance, because insurance laws and regulations in those jurisdictions are vague on the topic, and there is no case law there on the issue.30 31

While Europe’s insurance regulations at first glance indicate that a master global insurance program written in the United States would be perfectly acceptable, in reality there are some knotty problems making those global programs comply with local insurance regulations across the continent.

Under insurance regulations across Europe, which comply with the EU’s third non-life insurance directive, all EEA countries accept as valid an insurance contract written by a licensed insurer in another EEA country. This freedom-of-service insurance policy can be
The impact of global privacy laws on cyber risk mitigation

tied to a master global cyber policy written outside of the EEA, thereby eliminating the need for a non-EEA-based parent company to purchase local policies in every EEA country where the parent has cyber liability exposure. Likewise, in other jurisdictions outside of the EEA that bar non-admitted insurance, a local policy can be tied into a global master policy to provide the local operation additional limits and broader coverage terms on a difference-in-conditions or a difference-in-limits basis.

However, those insurance buyers are not relieved from the responsibility of ensuring that their global programs comply with the numerous different — and sometimes conflicting — insurance requirements in each EEA country. Rather than attempting to meet that daunting — and perhaps impossible — regulatory challenge, risk managers could guarantee their program is regulatory compliant by purchasing a local cyber policy in every EEA country where the parent company has that exposure. A risk manager then could tie the local coverage into a parent company’s master global program for additional limits and broader coverage terms, if necessary.

Failing to comply with local laws and regulations governing non-admitted insurance can be costly in many ways — including regulatory fines, unanticipated premium taxes and income tax assessments against the parent company — and jurisdictions around the world increasingly are looking for violators.

Those risks arise from a 2001 E.U. Court of Justice ruling in a nonlife insurance premium tax case that not only is precedential in Europe but also has influenced insurance regulators worldwide.

The case examined whether London-based Kvaerner P.L.C., which had covered a Dutch subsidiary under a global professional liability insurance program, was required to pay a premium tax in the Netherlands even though the coverage was not purchased there.35

The court ruled that Kvaerner — now TH Global Ltd. — was obligated to pay a premium tax on the portion of its global program that covered its Dutch risk.

The ruling has several implications for every multinational organization, whether it has operations only in Europe or globally.

In every EEA country where risk is covered under a master global program, the organization owes premium taxes, and regulators will seek them. However, a local broker or local insurer typically has to remit those. But since neither would be used in a global program, there is no mechanism to pay the premium tax, which then can lead to some serious problems:36 37

• If a global program underwriter pays a loss to a parent company rather than its foreign unit, those proceeds might be subject to taxation domestically and then again overseas if the parent moves the funds to its unit.

• A foreign regulator might bar the parent from moving funds to its unit if that transaction would violate the parent’s maximum allowable investment in the unit.

An organization that operates in a jurisdiction that bars non-admitted coverage but is covered by cyber insurance written elsewhere also gives up some important services. Insurers arrange and cover risk assessment, risk engineering, claims handling and loss forensics. But a non-admitted insurer cannot arrange for and cover such services where it legally cannot provide insurance.38 39

32. Kalinich.
33. Lindsay.
34. Lawson.
36. Lawson.
37. Keegan.
38. Beeson.
39. Longmore.
Data security experts do not like to use the word if. To them, a security breach is unavoidable.

Data security experts do not like to use the word if. To them, a security breach is unavoidable. It can be delayed, but at some point, the spate of hackers, motivated often by profit but also for political and other reasons, will find a way to penetrate any organization's system of riches — the personal information of thousands or millions of customers or clients.

Meanwhile, from the other direction, lawmakers in many countries — particularly in Europe — are examining adding an additional cost burden to organizations that suffer system security breaches. Breached organizations in many more countries soon will likely have to notify every customer and client whose data was stolen. That will come on top of the already steep cost of investigating a breach, updating system security, restoring data, potentially severe regulatory fines, business interruption and, in many cases, remedying the damage the stolen personal information has caused individuals.

Given the likelihood and cost of a data security breach, organizations around the world — as U.S. companies already are beginning to — might turn to cyber insurance to finance this risk. But a multinational company can expect coverage problems and other difficulties if it eschews locally admitted coverage and instead relies on a worldwide policy to cover its global cyber risks, since many countries bar non-admitted insurance.