PRIVACY & CYBERSECURITY

RISKY BUSINESS: PREPARATION, PREVENTION, REGULATION

DATA BREACHES: DEALING WITH THE AFTERMATH

Data breaches have become more and more common, to the point that companies essentially have to assume that sooner or later, they will experience one. That makes it critical to have a clear understanding of the regulatory requirements for notifying regulators and affected individuals in the wake of a breach. But the rules don't always make that process clear.

In the U.S., there is no single federal law covering breach notifications, but there are quite a few at the state level. Today, 48 states (in addition to the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) have some type of breach notification laws in place—with Alabama and South Dakota being the exceptions. "If a company experiences a breach of personally identifiable data about customers in one of these jurisdictions, it is obligated to notify those individuals, as well as regulators," says Jeffrey Poston, a partner at Crowell & Moring, co-chair of the firm's Privacy & Cybersecurity Group and a member of its Litigation Group. "A large company could easily be subject to dozens of state laws—if not all 48."

State notification laws typically define factors such as what constitutes a breach, what type of notice has to be given, and who must be notified—and these details can vary. For example, says Poston, "there are different triggers for having to notify the state attorney general. Some states say the breach has to involve more than 500 people; others say notifications are required based on the incident itself, regardless of the number of residents affected." The time frames for notifying individuals also vary—some states don't have a notification deadline except that it must be made without unreasonable delay; many states allow 45 or 90 days. Florida, with the strictest deadline, provides just 30 days for notice to be given.

Different states are likely to apply different degrees of scrutiny, as well. "Some state regulators just don't have the resources or the technological expertise to really mount a formidable investigation," says Poston. "Some are more aggressive than others—but, of course, that will depend on how many of the state's citizens are affected by the breach."

Beyond all those state laws, companies also need to be aware of a growing trend toward industry-specific federal regulations that include provisions covering data breaches. HIPAA has such notification requirements for the health care industry, and the Defense Contracting Agency has them in the DFARS (Defense Federal Acquisition Regulation Supplement) regulation. Even commercial agreements are starting to address the issue. "You may have to notify your business partners of a breach if you're handling data on their behalf or if you've got contracts that require you to notify them," says Poston.

Congress is aware of the challenges that companies face in trying to find their way through this thicket of notification requirements. A number of related bills have been proposed in recent years—including one in November 2017, the Data Security and Breach Notification Act. This legislation would preempt state laws and standardize notification requirements, provide a 30-day notification deadline, and call for prison sentences for those knowingly concealing a breach. However, these legislative efforts have so far failed to gain much traction—and for the time being, companies will have to navigate the nuances and variations across jurisdictions.

"You don't want to compound the problem by sending out an untimely or inadequate or incomplete notification to regulators and affected individuals." —*Jeffrey Poston*

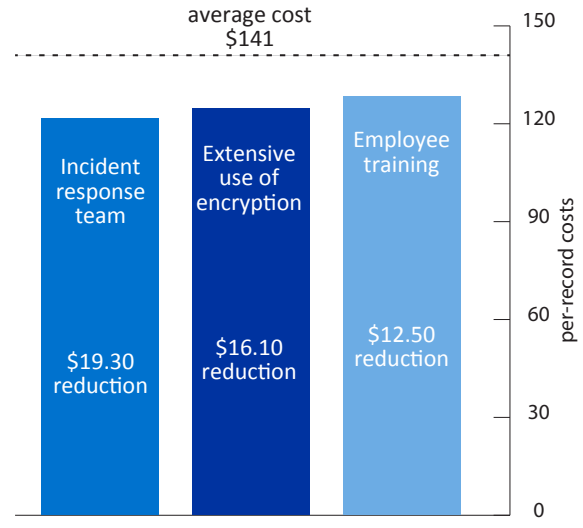
AN OUNCE OF PREVENTION

In this environment, companies should have a rigorous incident response plan in place. This plan should spell out how investigations and notifications will be handled and, as much as possible, try to anticipate problems that might arise. "As general counsel who have been down this road know, this can get complicated," says Poston. "You have to commence a privileged investigation right away, which typically involves very tricky forensic and technical information. It can take a lot of time and effort just to find out what data has been accessed or stolen and who has been affected."

Nevertheless, companies need to produce notifications that are both timely and accurate. "You've got just one shot at this," says Poston. "You don't want to compound the problem by sending out an untimely or inadequate or incomplete notification to regulators and affected individuals." Regulators will take a dim view of language that appears to be downplaying the problem, and if the notification (and related press releases) turns out to have significant errors, the company may have to re-notify everyone. "A breach is bad and embarrassing, but with today's news cycles, something else is likely to come along the next day

PREPARATION PAYS OFF

On average, a data breach costs a company $141 per compromised record. But research shows that certain activities can reduce those per-record costs.



Source: "2017 Cost of Data Breach Study," Ponemon Institute

A LONG TO-DO LIST

When a company experiences a significant cybersecurity breach, the range of necessary follow-on actions can be daunting. For example, legal departments will typically have to contend with:

- Deciding whether and when to provide notification to individuals and regulators, looking across dozens of state laws.
- Creating notifications that are timely and accurate.
- Communicating with external sources, such as media, law enforcement, and consumer-reporting agencies.
- Preparing statements, email notices, and personalized correspondence to reach employees affected by security incidents.
- Determining whether and how to provide post-incident assistance, such as credit-monitoring services or insurance, to affected individuals.
- Engaging a forensic investigation team covered by legal privilege.
- Assessing and addressing any criminal, employment, contract, or other legal issues arising from incidents that involve the conduct of an employee, vendor, or business partner.
- Defending against state and federal regulatory investigations, state attorneys general lawsuits, and individual and class action lawsuits arising from data and privacy breaches.

Later, when the crisis is under control, companies should conduct a "lessons learned" analysis of the incident and the response. This should focus on identifying potential improvements in privacy and data security—and the response plan itself—in order to reduce risk and limit the damage from future incidents.

that gets people's attention," says Poston. "You don't want to have to come back and re-focus the spotlight on yourself."

Response plans should consider possible litigation, as well as regulatory developments. With large data breaches, companies usually conduct an investigation to determine if a notification is necessary and, if it is, go through the notification process. But that may be just the beginning. "All of a sudden," he says, "you could have federal regulators opening up an investigation, state regulators opening up an investigation, and class actions being filed—and now you're in a three-front war. So you've got to be able to deal with each front in a way that doesn't jeopardize you on the other two."

With all these factors in play, response plans should be in place well before a breach happens. "You don't want to be reacting on the fly to a crisis," says Poston. "You want a plan that's been tested through dress rehearsals, fire drills, and tabletop exercises. Then, when there is an event, you have the muscle memory to react to it in an efficient, effective manner—without a mad scramble."

MEETING CLIENTS' EXPECTATIONS

Cybersecurity, a main concern for companies of all stripes, is of the utmost importance to law firms, where the protection of confidential client information is paramount.

Hackers, from lone wolves to nation-states, have figured out that law firms are a back door to the secrets of some of the world's top companies.

"Everybody is a target, no matter how big or how small, how important or unimportant they think they are," says Mark Sportack, chief information officer at Crowell & Moring. "Cyber is a scary thing."

So scary, in fact, that law firms must devote time, resources, and attention to making sure they are protected. "The only way to defend yourself in an environment with unknown, unseen risk is to have many, many layers of overlapping defenses," Sportack says.

RAMPING UP PROTECTIONS

"No law firm is ever fully prepared, and we are constantly benchmarking and looking to upgrade our protections," says Sportack, who runs Crowell & Moring's cybersecurity systems and strategy, adding that the ever-evolving nature of cyberattacks makes them a tough threat to effectively head off.

Crowell & Moring, like most law firms, takes cyber threats very seriously, viewing cybersecurity as a major new element of the attorney-client relationship. Sportack oversees a team that takes a multi-step process to safeguard the firm's network and sensitive data, working to ensure that its cybersecurity meets clients' exacting expectations.

First, Crowell locks down the computers it provides to employees so that nobody has local administrator privileges and therefore can't change the operating environment. "If you do that, you can address up to 80 percent of the risks you're facing," Sportack says.

Next, the firm requires that all remote access clear two levels of authentication. In addition, the firm locked away all administrator and other privileged access accounts to make sure they are activated only when specific operating environment changes are needed.

DELAY CREATES HACKING OPPORTUNITY

In addition, Sportack has a dedicated team available at all times to identify and fix security vulnerabilities as they occur. "You want to have a rigorous patch-management program because delay creates opportunity," he says.

The final piece in the protection pie is properly training employees about cybersecurity risks and how to deal with them. "The single biggest weak link in any given network is going to be the people," he says. A law firm might not be able to completely train user mistakes away, but Sportack says it can train them down to a minimum.

With the potential fines, investigation expenses, and reputational costs associated with data breaches, those response plans are likely to be well worth the effort. With the growing frequency and visibility of breaches, the public has become somewhat desensitized to news about security compromises. As a result, says Poston, "you have a chance of being forgiven by your customers if you experience a breach. But you have very little chance of being forgiven if you don't respond in an effective way to notify and protect them. If you don't act nimbly, it's not going to sit well with those individuals—or with regulators."

BRINGING HARMONY TO THE EU

In Europe, companies have been contending with a fragmented privacy and security regulatory landscape much like that facing U.S. companies. But that is about to change, when the EU General Data Protection Regulation goes into effect in May 2018.

For more than two decades, the protection of personal data has fallen under the EU's Data Protection Directive 95, which

"The only way to defend yourself in an environment with unknown, unseen risk is to have many, many layers of overlapping defenses." —*Mark Sportack*

THE SOFT UNDERBELLY OF THE SUPPLY CHAIN

As in any battle, the cybersecurity war has its hard and soft targets. Defense contractors have long been targets of hacking attacks and now have so many digital defenses that they are no longer worth the time and effort it would take for a successful breach. So hackers have turned their attention to the companies that supply the major defense contractors, in the hope that a successful breach in the supply chain will work its way back up into the defense contractor's network. This has national security implications, because the Chinese, Russian, and Iranian governments have been implicated in recent global cyberattacks.

Law firms face exactly the same risk. "Foreign nation-states are recognizing our clients as very hard targets," Sportack says. "They realize that in a lot of ways, we're an equally hard target. So now they're reaching into our supply chain. They're attacking companies two levels removed in the chain of commerce from their actual target."

TAKING THE FIGHT TO THE SUPPLIERS

To counter that threat, Crowell & Moring has begun systematically vetting all its vendors to make sure that they meet its strict cybersecurity requirements—standards that seek to meet the demands of the firm's clients. "We are taking the fight to them," Sportack says.

All new vendors must pass the cybersecurity test or they are turned away. The law firm is also starting to hold existing vendors to the same standards. So far, roughly one in three existing vendors isn't making the cut and has to be dropped.

All law firms now recognize that they (and therefore their clients) are vulnerable to cybersecurity attacks. A 2017 survey of more than 200 law firms by LogicForce found that 80 percent are not vetting their third-party vendors' data practices. That can and will change. By definition, no cybersecurity system is impenetrable. But Crowell & Moring is working every day to make that system more secure.

provided some harmonization of regulations. However, EU directives provide only a regulatory framework with minimal rules, which then need to be incorporated into national laws in member states. As a result, those laws have often diverged, leaving significant variations in regulations across the EU.

"Spain has had very strict data protection regulations, and regulators in France, the U.K., and Germany have been very active," says Maarten Stassen, a senior counsel at Crowell & Moring and a member of the firm's Privacy & Cybersecurity Group. "On the other hand, in other countries such as Belgium, the data protection authority had a more advisory role but could not impose any sanctions in case of a data breach. These different approaches made it quite challenging for companies to be compliant."

The GDPR essentially replaces the EU Data Protection Directive. As a regulation, it will be directly applicable in all EU member states as of May 25, 2018. Individual countries have leeway to make some adjustments, but "in general there is a much more harmonized approach," says Stassen. Under the GDPR, there is still no single enforcement authority. Instead, each country has an independent supervisory authority that hears complaints and applies sanctions. The activities of these various authorities are coordinated by a European Data Protection Board that helps ensure consistent enforcement across the EU.

Along with the harmonization of regulations, the GDPR was developed to help "move privacy and the protection of personal data up higher on companies' agendas," says Stassen. To that end, the regulation provides significant penalties for noncompliance and data breaches. These can be as much as 4 percent of a company's annual revenues, or up to €20 million, whichever is higher. While those top fines might not be levied immediately, the risk is significant, and "these potential fines have succeeded in getting the C-suite's attention and getting this on boards' agendas," Stassen says.

Much of the GDPR is based on the previous EU directive, so the concepts behind it are familiar to companies doing business in Europe. But there are some key changes. In addition to the substantial fines now on the table, for example, the GDPR requires companies to notify authorities of a breach—a requirement familiar to U.S. companies but not covered under previous regulation. It also requires that such notification happen quickly—within 72 hours of a breach being discovered. "In general, the big differences are that the GDPR makes companies more accountable and requires them to demonstrate to authorities that they are in compliance," says Stassen.

These new rules do not apply only to European companies. U.S. companies with a physical presence in the EU will also need to comply. What's more, the GDPR will also apply to com-

THE EU'S BILL OF DATA RIGHTS

The GDPR grants a number of rights to individuals, or "data subjects." Companies are obligated to respect those rights in their handling of data.

- Right to information—the right to receive detailed information about the processing of personal data collected from the data subject or from other parties.
- Right of access—the right to obtain confirmation from the controller—the party that determines how the data will be used—as to whether the subject's personal data is being processed and, if so, the right to access and receive certain information about personal data stored by the controller.
- Right to rectification—the right to rectification/correction of personal data that is inaccurate, and to have incomplete personal data completed.
- Right to erasure ("right to be forgotten")—the right, under certain circumstances, to have personal data deleted.
- Right to restriction of processing— the right to require that the use of personal data be limited.

"If the people in the business don't know that's a requirement, then they can't comply with the regulation. So these things need to be built into business processes." —*Maarten Stassen*

panies located in the U.S. that actively market to EU citizens and gather their personal data or monitor their behavior within the EU, as well as to companies that process data for these companies.

ADAPTING TO THE GDPR

In practice, the GDPR will require companies to make some operational changes. For example, it guarantees the "right to be forgotten," meaning individuals will have the right to request that companies in specific cases erase personal information from company records. While EU individuals already had significant data protection-related rights, it is likely that they will now exercise those rights more often, and companies will need to have processes in place to handle that. The regulation also raises the bar on how data usage consent is gathered from individuals. Consent, it says, must be informed, given freely, and apply to a specific purpose. Furthermore, it must be given in an unambiguous way. Therefore, companies will need to find ways to have individuals take "affirmative acts," such as opting in to provide consent. "Companies will need to demonstrate that individuals are actively making an informed choice," he says.

Among other things, the GDPR requires companies to keep records of data processing activities. This includes identifying the personal data they have, explaining how data privacy will be ensured, and justifying why they need that data—information that is used to show regulators that the company is in compliance.

Companies also need to conduct a data protection impact assessment (DPIA) before beginning any processing operations that pose a significant risk to individuals' information. This might be required when creating new customer profiles, using a new technology, or starting a program involving the monitoring of public areas on a large scale. If the assessment shows that risk would be high and requires actions to reduce that risk, companies will need to consult with the relevant supervising authority before proceeding and clarify how that risk will be mitigated.

The changes necessary to meet these kinds of requirements will be felt throughout the company. With the DPIA, for example, compliance is not just an issue for the company's law department. "Everybody in the company needs to be aware that when they are at the start of a new project or initiative that is going to do something new with personal data, they need to consider whether to do a data protection impact assessment," says Stassen. The same is true of the data breach notification rule. "If the people in the business don't know that's a requirement, then they can't comply with the regulation," he says. "So these things need to be built into business processes."

Effective GDPR compliance, Stassen continues, requires a "change of mind-set" in the company. That can mean adopting new policies and procedures, implementing new technology, and providing training to staff to increase GDPR awareness. Operations are usually relatively siloed at most companies, but data moves horizontally through the organization. "The GDPR forces you to look at the data flow beyond your silo and think about the whole business," he says. "Companies are going to have to look at their business processes through the lens of data privacy."

BRIDGING TWO WORLDS

The GDPR continues the EU's prohibition against transferring personal data outside of the EU unless certain conditions are met. But for companies in the U.S., the EU-U.S. Privacy Shield program provides a way to keep the data flowing.

Put in place in May 2016, Privacy Shield is a framework in which U.S. companies publicly certify that they will follow EU data privacy regulations, thereby gaining approval to move personal data from the EU to the U.S. Some observers have said that such programs are often little more than a "check the box" exercise. But that's not the case with Privacy Shield, says Crowell & Moring's Maarten Stassen. For one thing, he explains, "companies that sign up are really putting themselves on the radar of EU and U.S. regulators."

Those regulators are taking an active approach to the program. EU data privacy authorities have shown in the past that they are willing to follow up with companies to explore the processes being used to protect data. In addition, in September 2017, three companies agreed to settle charges from the U.S. Federal Trade Commission that they had misled consumers about their participation in Privacy Shield. A commission official noted the agency's "commitment to aggressively enforce the Privacy Shield frameworks," adding that participating companies "must keep their promises or we will hold them accountable."

Privacy Shield may not be perfect, says Stassen, "but it's a reasonable solution, and companies in the program need to make sure they have the compliance processes in place to back up their certification."