HEIDRICK & STRUGGLES

Protecting customer information

Can you afford not to have a Chief Privacy Officer?

by Julian Ha, Esq.

In the wake of unprecedented thefts of personal information, companies in the transaction processing and information services businesses that have not established the role of Chief Privacy Officer (CPO) should do so before they become the next victims – and perhaps put their reputation and their business at risk. The duties and responsibilities of CPOs in businesses whose lifeblood is information go far beyond merely guarding marketing information and monitoring compliance. Understanding the complex demands of this role and finding the right people to fill it should be a high priority for information companies that want to maintain public confidence and protect shareholder value.

Periodic, high-profile security breaches at retailers, information companies, credit card companies and banks over the years have steadily raised concern among consumers, online shoppers, e-commerce merchants, retailers and legislators about protecting the public's personal information. Even during lulls in such incidents, companies and the public know that the potential for further problems remains. Moreover, changing regulations oblige transaction processing and information companies to disclose such breaches, further exacerbating public concern and undermining company images and the business. Although some companies – largely those that have been victimized – have shored up their privacy operations by hiring CPOs, many have not. It's a dangerous gamble, where traditional calculations of return on investment don't apply.

The bet, rather than a simple trade-off between a salary and bottom-line benefits, is no less than the company's reputation and the business itself. In the face of these challenges, progressive leaders of transaction processing and information companies are proactively working to put their companies at the forefront of privacy protection. Although they are confident that they have the latest in technology, they know that the thieves are still lurking out there. Further, they know that not all of their vulnerabilities are technological, and they are determined to see that no catastrophic breaches of privacy occur on their watch.

From extensive conversations with these leaders, we have found that they are trying to make privacy a central concern at all levels of their organizations. They are looking outside of their industries to find talent that can comprehensively address these issues. Above all, they understand that privacy is their business, and they see the current climate as an opportunity to strengthen their privacy programs and advance their business goals by demonstrating real leadership.

Drawing on these in-depth conversations with executives and our extensive experience in the industry, we provide here a picture of the CPO role in transaction processing and information services companies, identify emerging best practices, and offer some recommendations about finding the right people to fill these highly complex and demanding positions.

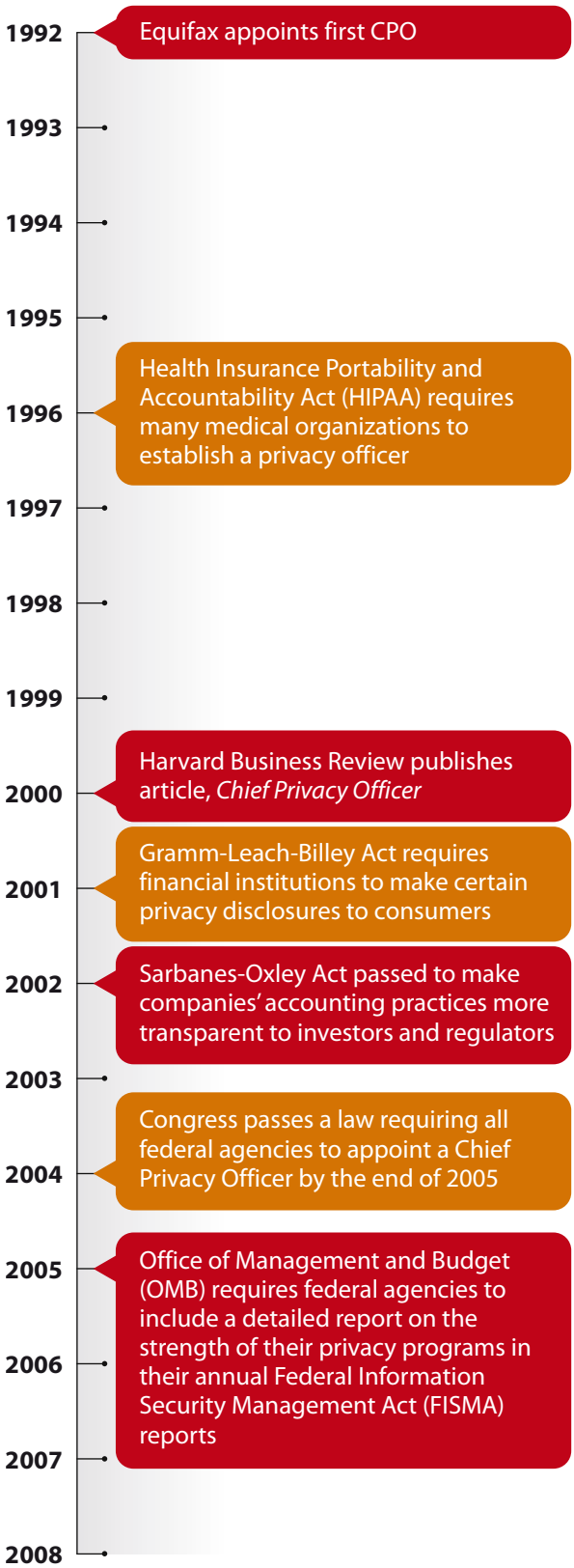
Rapid evolution

Interest in the role of CPO isn't entirely new – the first CPOs appeared in the early 1990s. But between 1998 and 2001, more than 100 companies, including IBM, AT&T, and American Express, appointed CPOs. Faced with Y2K, however, many companies began diverting money away from privacy and toward issues of continuity. The events of 9/11 intensified this concern, as more and more companies examined their security policies to make sure they could continue to operate in the event of a disaster or an IT catastrophe.

Today, a combination of public concern, increasing state and federal legislation, and highly publicized losses of personal data has once again put privacy concerns on the front burner. Every federal agency, regardless of size or function, must employ a chief privacy officer as well as use an outside auditing firm every two years to ensure compliance with the nation's privacy laws. And Sarbanes-Oxley has put additional burdens on CEOs and boards, putting the responsibility for Section 404 compliance squarely on their shoulders. For transaction processing companies, that means putting the processes that account for the bulk of revenues under the SOX microscope – a unique opportunity to leverage privacy programs in the compliance effort.

Government agencies as well as companies know that what is at stake for them in privacy issues is the most valuable commodity of all: the trust of the people they serve. Unlike government agencies, however, information companies that lose that trust harm their bottom lines and risk their very survival. They are vulnerable to lawsuits, loss of market share, and decline in share price. Even in the absence of a lawsuit or sanctions, the negative publicity arising from the misuse or even the alleged misuse of personal data can put a company's brand in jeopardy and severely damage its value. When evaluating preemptive investments in privacy protection, executive management should keep these considerations top of mind, forgoing traditional financial justification in terms of costs and benefits and instead adopting a more actuarial approach that takes into account risk, exposure, and material loss. When they do, they will likely find that the scale of potential value destruction more than justifies the hiring of a CPO.

timeline
making privacy a priority



From preventing the destruction of value to creating it

Recognizing the value of a CPO, progressive companies with whom we have talked take the argument one step further. They see privacy protection not just as a tactical matter but as a strategic issue. They believe that by leading the way in privacy protection they can enhance their reputations with customers and consumers and ultimately grow market share. Further, the right CPO, rather than acting as a mere roadblock to new initiatives, services and products, can also help optimally balance the costs and risks of privacy policies. The CPO can also ensure that the company's interests receive a fair hearing in the arena of public policy. As these forward-looking companies realize, the job of the CPO is not only to prevent the destruction of value but also to contribute to its creation.

To this far more strategic and complex role, a prospective CPO must bring the same qualities of leadership and business acumen that boards and CEOs expect of other C-level executives. Ideally, the CPO should be one of those executives with the ability to "change the game" and give the company not just parity with other companies in privacy matters, but advantage over them – in cost effectiveness as well as in rigor and innovation.

In addition to being a leader and a business innovator, the CPO must also be able to take responsibility across a broad range of areas, including:

Privacy policy

The CPO is responsible for developing and implementing privacy policy – how information is circulated, used, and by whom – across the organization. The CPO must define company expectations regarding the level of exposure and risk the company is prepared to take, since absolute privacy, like absolute security, is impossible to reach and exponentially costly to approach.

Privacy-risk assessment

The CPO, often upon installment, may conduct an assessment of the risk entailed by the company's privacy practices as well as the nature of the information the company collects. Where might the company be at risk and what is the nature and magnitude of the risk – bad publicity, damage to the company's reputation, lawsuits, regulatory sanction?

Sarbanes-Oxley/404 Compliance

As compliance becomes an increasing source of concern to CEOs and boards – and increasingly costly – the CPO should use the experience gained in scrutinizing processes for privacy to help streamline SOX compliance, making it less likely to turn up material weaknesses and reducing its cost.

Privacy audit

Privacy issues may change as changes in the business occur; employees may relax their vigilance; new technology may introduce new ways of handling information. For all of these reasons, CPOs should regularly assess all company operations that involve personal consumer information, making privacy an ongoing process – not a one-off report – throughout the company.

Privacy training

The CPO, often in conjunction with Human Resources, must see to it that employees throughout the organization are educated about company privacy policy, trained in standard operating procedures and, where appropriate, evaluated on their performance. Alliance partners and other members of the company's network may also require education about the company's policies and procedures.

New initiatives assessment

The company must have a process in place for assessing privacy issues raised by new products and services as well as acquisitions, joint ventures, partnerships and strategic alliances. To be effective in this area, the CPO must thoroughly understand the company's business and numerous business disciplines including marketing, product development and business strategy.

Data security

The CPO must thoroughly understand technology, including technological safeguards as well as threats. Moreover, because the structure of the transactions business often involves loose federations of companies, the outsourcing of many steps in the transaction process, and a lack of uniform standards among the many parties to transactions, the CPO must strive also to ensure data security along links in the chain that lie outside the company's control.

Data ownership

Because transaction processing companies do not own the data they handle, they must be vigilant at all times about working within the bounds of permissible use. The CPO should not only understand and disseminate those operating rules but also champion a culture of responsibility and integrity in the absence of which the rules may have less force.

Legal and regulatory policy: Today's CPO must understand the current state, federal, and international legal and regulatory climate and make sure the company is compliant with all relevant standards everywhere it operates. Beyond compliance, the CPO must understand how regulation affects a company's domestic and global business lines, and how it is likely to evolve.

Lobbying

Because the form that regulation may take has profound consequences for the business and because no one understands the unique operating demands of transaction processing and information services better than the companies themselves, the CPO must be able to make sure that the company's voice is heard. This may involve forging alliances with other industry players, working with industry leaders, and making effective use of government relations resources.

Ensuring best practices

Ultimately, the success of the CPO – and therefore the successful protection of the company's reputation and business – depends on how the role is integrated into the organization. In the relatively short time since the position first appeared, a number of best practices have already emerged:

Make sure the reporting structure gives the CPO the requisite power

Often, for the overall good of the company, the CPO must make some tough calls – quash a new product that lacks sufficient safeguards, call

attention to technological shortcomings, insist on privacy considerations across functions – that ruffle powerful people in the company. Unless the CPO has the full backing of the CEO and board, reflected in the reporting structure, he or she will be powerless to exercise the independent judgment necessary to fulfill the responsibilities of the role. In some companies, the CPO reports directly to a Privacy Committee of the board, in others, directly to the CEO. In companies that regard privacy as part of security and risk management, the CPO should be on at least an equal footing with the senior risk management executive and, in any case, still report to the board or the CEO. Anything less than having a powerful line into the Board or the CEO can seriously dilute the ability of the CPO to make the objective judgments necessary for adequately protecting the company. It is potentially fatal, for example, to subordinate the CPO to the CIO in the mistaken belief that privacy is a technological issue only. It also sends the message that the company regards the position as window dressing. And it makes it harder to attract a multi-talented person with the experience and knowledge to handle all of the role's disparate responsibilities.

Make privacy part of the fabric of the organization

From business strategy to operating procedures, from the boardroom to the operations center, privacy should be the concern of everyone in the organization. Scrubbing for privacy should be an integral part of designing a new product, formulating a new strategy, introducing a new technology, or interacting with partners. More than simply a policy, privacy should be a mindset, a core value deeply embedded in the company and wholeheartedly subscribed to by all employees.

Keep the focus on business

While maintaining data privacy and ensuring safeguards are essential elements of the CPO's role, they are not synonymous with it. Remember that the critical purpose of having a CPO is to enhance the business of the company, protect its reputation, and maintain and create shareholder value. A purely technological rationale for installing a CPO is likely to omit the proactive business focus that a CPO must take.

The CPO should offer solutions, not roadblocks

The CPO's role is not that of a cop pointing out violations and telling people "no." In fact, the best CPOs focus not on problems or reactive fixes, but on preemptive and proactive solutions. If a new line of business, a new technology or an operating procedure could compromise privacy, the CPO should work closely with other stakeholders to try to reap the business benefits of the innovation while staying within the bounds of policy. The best CPOs are savvy negotiators and good mediators who can bring stakeholders to a mutually beneficial agreement. Above all, the CPO must be able to make a business case for the protection of information.

Finding the right person for the role

How difficult is it to find someone who can shoulder the multiple responsibilities of the CPO role and fully deliver on its benefits to the company? On the one hand, the role has emerged so recently that few people have experience as CPOs.

On the other hand, because the job involves such a broad range of skills and knowledge, potential CPOs

may be drawn from many backgrounds, especially business and professional services, but could also be drawn from other areas, including law, government affairs, technology, auditing or intelligence.

Apart from the candidate's background, however, transaction processing and information companies should look for the same qualities of leadership that they look for in their other C-level executives: subject matter expertise, impeccable communication skills, an authoritative presence, business vision, and an unflinching willingness to make independent, objective judgments. Equally important, the CPO must not only subscribe to the highest ethical standards but also be able to inspire others to adhere to them as well. Ultimately, protecting the company is not only a business necessity, but also an ethical imperative.

After all, it's not about data, it's about people's lives and livelihoods. Candidates who combine the requisite business acumen, ethical ballast, and skills relevant to the intricacies of privacy may be hard to come by, but recovering your company's reputation can be even harder. ■

Julian Ha

Julian Ha is a Member of the Legal, Risk, Compliance & Government Affairs practice at Heidrick & Struggles. He focuses on recruiting senior executives in technology, financial services, energy and healthcare industries in which privacy protection is a critical business issue. Prior to executive search, Julian practiced corporate and securities law and was a senior operational executive for a financial data provider.

jha@heidrick.com
+1 (202) 974 6088

HEIDRICK & STRUGGLES

Heidrick & Struggles is the premier provider of senior-level Executive Search, Culture Shaping and Leadership Consulting services. For 60 years, we have focused on quality service and built strong leadership teams through our relationships with clients and individuals worldwide.

www.heidrick.com

201303JNTSRG1