In Search of the Privacy Officer
CSI December 2004 Alert
Rebecca Herold, CISSP, CISM, CISA, FLMI
October, 2004

So, what about this emerging Chief Privacy Officer (CPO) position that was ballyhooed so much around 2000 to 2001? Has this new position really caught on like wildfire as was widely predicted? In 2001 Forrester issued a report asserting the establishment of a CPO would be the best way to effectively manage all organizational privacy issues and help to mitigate privacy risks and liabilities. They recommended the position to be at a high enough level to have a wide view of the entire business enterprise activities, and to also have the authority to implement and enforce activities to ensure compliance with privacy policies, laws and contractual requirements. Of course this makes sense; we heard similar, good, logical ideas when the role of the Chief Information Security Officer (CISO) emerged.

The U.S. Government's CPO Point of View…

So, how does the CPO landscape look today? Before jumping to any conclusions, and even before Googling to gather information about privacy officer trends, I first searched through the Department of Labor (DOL) web site. I could not find the term "privacy officer" used on the DOL site; however, they do reference "compliance officers" which has grown to encompass privacy responsibilities for many organizations. The DOL statistics for these compliance officers include:

- 2002 employment: 158,000
- Projected 2002-12 employment change: About as fast as average
- Most significant source of training: Long-term on-the-job training

Let's Check Some Other Sources…

After not finding much information at the DOL to help me in my quest for some solid numbers and trends, I contacted a variety of privacy organizations and executive search firms who specialize in information security and privacy positions. These included the following organizations:

- 12 information security, audit and privacy executive search firms
- Robert Ellis Smith, privacy writer, author of Ben Franklin's Website, editor and publisher of The Privacy Journal, and others.
- Dr. Larry Ponemon from The Ponemon Institute
- Privacy and American Business (PandAB)
- International Association for Privacy Professionals
- The Organization for Economic Cooperation and Development (OECD)
- The American Marketing Association
- The Institute of Certified Professional Managers
- Electronic Privacy Information Center (EPIC)
- International Public Management Association for Human Resources
- National Management Association
- Financial Executives International
- Financial Management Association, International
- Society for Information Management

I received replies with information from Robert Ellis Smith, Larry Ponemon, the OECD, PandAB, and Talent Scouts, Inc. Most of the management and executive associations

responded that they did not have any statistics on CPOs. I did not hear back from most of the others.

The OECD's Point of View…

The OECD has not done any specific studies into the trend worldwide for CPOs; they "primarily deal in macro-economic indicators." However, they do have some interesting links that, while not directly specific to the role of CPO do contain some general insight into their work and recommendations for information privacy, security and human resources in science and technology positions. See:

- Privacy Main Web Site
  http://www.oecd.org/department/0,2688,en_2649_34255_1_1_1_1_1,00.html
- Culture of Security Web Site
  http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
- Human Resources in Science and Technology
  http://www1.oecd.org/publications/e-book/92-2003-04-1-7294/A.9.1.htm

Privacy and American Business's (PandAB) Point of View…

PandAB did not have any recent numbers for named CPOs. However, for comparison it is worth looking at a survey they did in 2001, along with their predictions, and see where we're at today. At that time 294 people belonged to PandAB, the Association of Chief Privacy Officers (ACPO) and the Privacy Officer's Association (POA). All three of these have since merged. Of 102 privacy officers completing the survey, 25% had a law background, 18% had a management background and 17% had a marketing background. The survey director Alan F. Westin, Professor Emeritus of Public Law and Government at Columbia University and president of the Center for Social & Legal Research, noted at the time, "The rise of the corporate privacy officer shows that corporations are beginning to take privacy seriously." At that time Westin put the number of privacy officers within the U.S. at around 500.

The Ponemon Institute's Point of View…

Dr. Larry Ponemon and the Ponemon Institute provided the following information gathered from the Ponemon Institute's benchmark database of corporate privacy practices. The information was accumulated using benchmark surveys in 2003 and 2004 from 129 large corporations or governmental organizations; 69 of the organizations are in the Fortune 500. Additionally, the Ponemon Institute does a yearly salary survey on privacy professionals in partnership with the IAPP. In 2003 and 2004 they collected data including information about title, role and reporting structure. Dr. Ponemon provided the following table showing analysis of the collected information.

	Fortune 500*		Other Companies#		Total Benchmark	
Based on Ponemon Institute Benchmark Results	Freq	Pct %	Freq	Pct%	Freq	Pct%
Professionals currently estimated to have the title "Privacy Officer", or otherwise have a position dedicated to addressing privacy	48	70%	24	35%	72	56%

issues, within the U.S.?						
Professionals currently estimated to have the title "Privacy Officer, " or otherwise have a position dedicated to addressing privacy issues, worldwide?	40	58%	14	21%	54	42%
2005 Estimate (based on 9% net change between 03 and 04)	52	75%				
2005 Estimate (based on 11% net change between 03 and 04)			27	40%		
*Based on 69 companies #Based on 68 companies						

Robert Ellis Smith's Point of View…
Robert Ellis Smith also provided good insight into the estimates for how many CPOs currently exist within some of the more privacy-aware industries. As he points out, each healthcare organization, or more specifically, each organization that qualifies as a covered entity, must have a privacy officer to comply with HIPAA. I checked with multiple agencies and departments within the Department of Health and Human Services (HHS), and out of the dozen or so I spoke with, and unfortunately they could not provide any specific numbers. With regard to other industries, Smith points out that about six states have designated CPOs, and probably every federal agency has a CPO. In the private sector, Smith estimates there are around 400 non-healthcare companies that have CPOs, and some of those have more than one privacy professional in the company. Smith's final estimates are that there are 500 CPOs in the private non-medical sector in the U.S., 2500 (full and part-time) in the healthcare sector, 150 in the governmental sector in the U.S., and 200 in government and private business in Canada.

Executive Recruiters' Points of View…
I figured I should be able to obtain some additional information, particularly with trends, from executive search firms that specialize in placing information security and privacy professionals. So, I asked 12 information security and privacy professional recruiting organizations to respond to some questions regarding staffing for privacy officer and related positions. One of the firms, specializing in placing privacy professionals, Privacy Leaders, Inc., responded to me in September that they could provide the information, but when I followed up with the company in October it appears they are no longer in business. Does not appear to indicate a growing trend in privacy positions, does it? I heard back from one organization; Brian Hunter with Talent Scouts Inc. responded that in 2003 he had zero privacy officer openings, but that this year he had filled two privacy officer positions; one in the financial industry and one in the healthcare industry.

Since only one of the recruiting agencies had any statistics they cared to share, I checked on monster.com on October 31 (I figured the timing would be appropriate for the sound of the site) to see what I could find there. Since I'm seeing many of the responsibilities for

privacy going to compliance officers, I included that term within my search, along with privacy officer and information security officer, to serve as a point of reference. Here's what I found:

- "Privacy Officer" had 13 listings
- "VP Privacy" had 67 listings
- "Compliance Officer" had 314 listings
- "Information Security Officer" had 21 listings

What Does This Mean…If Anything?

So, what does all this mean with regard to the growth, or shrinkage, of the number of CPOs? I needed to draw upon even more sources. While attending multiple conferences, monitoring many privacy mail lists, and reading the newsletters and other communications from the CPO associations to which I belong, it confirms to me that most of the existing named CPOs are lawyers or from the marketing areas. It's interesting to me to read multiple articles about CPOs and discussions about the challenges they have to keep up with all the new privacy enhancing technologies, and to understand how information security fits in with all the wide range of privacy issues. Why is this anything new? Security has always been necessary to help ensure privacy, even though privacy is not always an after effect of security. Hmm…is a CPO necessary to do these things, or can they be incorporated into existing positions? Certainly in the industries that have legislated privacy officer positions and responsibilities, a CPO is necessary. And, in large organizations that handle much personal information a CPO may be necessary. The key determining factor is the organization itself, and the wide spectrum of privacy risks that the organization faces.

Precise estimates of the number of corporate privacy officers are difficult to discover. Privacy officers have a variety of titles, such as chief privacy officer, privacy manager, and so on. And, as the 2001 PandAB survey revealed, a significant number of people responsible for privacy have another primary job responsibility, such as general counsel, compliance officer, or chief information officer.

Is There a Typical CPO?

Of course, there are many other responsibilities that should be addressed by someone responsible for privacy governance within an organization. At a high level some of these responsibilities should include:

1. Oversee of the use of privacy enhancing and inhibiting technologies
2. Keep up with new and changing privacy laws and regulations in all geographies where the company does business
3. Manage privacy policies and procedures
4. Oversee customer relationship management and the related privacy issues
5. Ensure personal information inventories are created
6. Track transborder data flows of personal information
7. Ensure privacy education to personnel and consumers

Some organizations in multiple industries have assigned the privacy responsibilities to compliance officers, in addition to trying to manage organizational privacy programs by a

central privacy council or committee; some with great success and some with great disappointment.

Many, if not most, organizations are trying to keep headcount down while assigning more responsibilities to existing positions; one of these responsibilities being that of privacy. This may or may not be successful depending upon the organization. More and more information security officers are becoming more engaged with the privacy program and activities. This is a good trend; it's a shame they so often were left out of the mix to begin with. Organizational leaders need to recognize the role information security leaders play in promoting and supporting privacy initiatives…privacy is certainly not just solely a legal or marketing issue.

Responsibility for Privacy Must Exist

Organizations must realize privacy is much more than just a legal issue. Besides privacy law requirements, privacy is also a marketing differentiator to organizations. Privacy is a component of compliance issues, customer and public relations, and information technology. Organizations are starting to involve IT into more privacy initiatives because of the significant importance of IT to ensuring privacy. Finding one person to address these wide ranging privacy components is such a challenge to some companies that creating a privacy council to address privacy concerns and distribute the various areas of expertise (law, marketing, public and customer relations, IT and business operations) among the council members is an alternative worth considering.

Whether or not organizations create a specific position responsible for privacy, or decide to govern privacy by council, they need to keep in mind the following:

- The highest executive management must be supportive of privacy initiatives.
- Creating and implementing privacy policies is a much more complicated task than it may seem.
- Privacy issues and policies must be effectively communicated.
- If governing privacy by committee, the committee must be well organized, consistent and have allocated time to be successful.
- Multiple IT issues are involved with privacy compliance, such as data retention, access controls, data flow analysis, and privacy enhancing technologies to name a few.
- Privacy must be built into new and updated processes as early as possible in the development process.
- The success of the privacy program will depend upon how high up in the organization the CPO, and/or privacy council members, are placed.
- The personal skills of the privacy officer are important to the successful implementation of a company's privacy policy; a privacy officer has to be able to work closely with legal counsel and understand legal issues, understand technical issues, be able to identify privacy priorities of the organization, and mobilize the organization to respond.

Companies that cannot figure out where to put a privacy officer in the organization would be better off starting with a privacy committee/council than taking chances with their privacy

obligations and incurring the costs of indecision by not assigning responsibility to anyone. Even if the numbers of CPOs have not reached the estimates made a few years ago, privacy continues to grow in importance and must be addressed by organizations in some manner by some one.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.

