Data protection surgery

Privacy experts and practitioners from T-Mobile, JPMorgan Chase Bank, the International Association of Privacy Professionals (IAPP), and *Privacy Laws & Business* provide the answers to some of the key privacy management issues affecting multinational organisations.

At our Annual International Conference in July, we gathered together a panel of privacy experts to share their experiences and thoughts on a range of privacy topics, including: what qualities do you need to be an effective chief privacy officer; how do you get buy-in from the board; and what steps should you take to cope with a media crisis?

What sort of preparation or background is needed for the role of Chief Privacy Officer?

Trevor Hughes, Executive Director, IAPP: The IAPP did a study with the Ponemon Institute earlier this year, looking at the profession of privacy in the US. I was interested to see the diversity of backgrounds coming to the privacy profession. Clearly there were many lawyers and attorneys in the privacy field. But there were also people with a Masters in business, marketing backgrounds, and some with public relations backgrounds. One of the struggles that chief privacy officers (CPOs) have in larger organisations is that all of those aspects are encompassed into the role of the CPO.

I don't think there is necessarily a single career path that would suggest success as a CPO. Depending upon the company and its needs, different experiences might play better. In a regulated industry, clearly an attorney might be a better choice for CPO, whereas in a consumer marketing company, someone from a PR/marketing background might be a better choice. A company about to be legislated out of existence might want a government affairs person as the CPO.

Martin Hoskins, Data Protection Manager, T-Mobile UK: I think there are four types of experience that are useful to have in our position. The first type is to be the sort of person where you don't have to worry about the law. You don't have to worry about each precise letter, comma, full-stop, or semi-colon. What's far more important is the ability to apply common sense to everyday problems.

Third is the ability to develop a constructive working relationship with the regulators. We have to accept that we are in a marathon not a sprint. We are going to be working with these people for a long time, so the sooner we can buy into their mindset, or get them to understand ours, the better.

The final and one of the most important qualities that someone needs to have is the ability to sometimes give in, and know when it's appropriate to fight another battle. Sometimes it is simply not worth fighting the point and better to look at more pressing problems.

> "develop a constructive working relationship with the regulators...We are going to be working with these people for a long time..."
>
> **Martin Hoskins, T-Mobile**

How do you get your board of directors to take privacy issues seriously?

Martin Hoskins: I find that one of the easiest ways, if I'm having a particular problem or issue with someone, is to invite them to make their comments in writing and point out that they will be personally responsible for the consequences of any problems that happen as a result. It tends to focus minds quite a lot. It's amazing how many times people back down.

It's also very much a business decision. Everybody in business has to make a judgment because we can't be as conservative as some of the legal advice that comes in. It's a matter of knowing when one can take a calculated risk – knowing full well that every now and then you're going to get it wrong, but most of the time you're going to get it right.

Valerie Taylor, Consultant, Privacy Laws & Business: I think it is important to make sure you have a two-way dialogue with the business area. You can't go in and dictate to a business area what they must do. You really have to talk to them and make them understand. One way is to try and relate privacy requirements to them as individuals. That very often focuses the mind.

Melonie Shilito, VP Data Privacy Officer, EMEA, JPMorgan Chase Bank: Try and relate compliance issues with damage to the business, the brand and the impact that failing to comply will have on customers. From a marketing point of view, you can demonstrate the bad will that could be generated if things go wrong, the damage to the bottom line and the impact on your brand.

Fortunately, in a way, there have been a few relatively high profile cases where things have gone wrong. Sometimes you can use those to say: "Look at company X and see how this went around the industry press – we don't want to be in this position do we?" That can help to focus peoples' minds.

Trevor Hughes: As long as you are demonstrating the risk associated with a lack of privacy compliance, you'll always be a cost centre, a place that is expense driven in the organisation. And that's okay, because there are risks associated with complying with privacy standards, but you will always be a cost centre.

Upper management will always look at you on the expense side of their balance sheet and not on the revenue side.

Another way is to show the return of privacy. That is harder to do, and has not entirely proven successful, but there are encouraging suggestions in the marketplace right now. An example is Microsoft who recently appointed Peter Cullen as their new chief privacy strategist. Peter Cullen comes from the Royal Bank of Canada (RBC) where he was at the vanguard of privacy as an ROI [return on investment] driver. He was proving the value of privacy to the customers of RBC. He made privacy part of the Royal Bank brand. In fact, in some of their consumer marketing campaigns, they really highlighted their higher privacy standards and then met those standards.

Microsoft hired Peter and ostensibly, or at least what I take from that, is that Microsoft is not hiring a police officer to sit within Microsoft and make sure there is strong compliance and risk management - although that is part of the job - they want him to come in and really prove the value of privacy as a revenue generator.

So I think you sell it to management in two ways. Show the downside and risk potential and make sure business units comply. But if you can, you also show the upside potential: privacy as polish on your brand, how it can help you improve customer relationships.

Martin Hoskins: It's also about how you can buy into the corporate ethics, knowing full well that there may be horrendous things going on that will take a long time to change. It's far better to change things gradually, rather than make a pain of yourself in the first couple of months and then find that there's a great big wall of resistance every time someone comes along with a project.

It's a matter of building long-term relationships within the company itself, and doing things gradually rather than very quickly. One of the problems with doing things quickly is that if you're not careful you can inflate people's expectations and you can then get inundated with requests for all types of work that you simply can't cope with.

So, sometimes it is useful to keep a low profile so that you can get on with the more significant strategic issues.

What systems are there for charging out the data protection department's time to other business areas?

Valerie Taylor: I have experience of three different ways of charging. One is a basic way of the whole cost of the data protection function being covered by the business generally as an overhead. In a way, that makes life easier if you've got the right number of people, a team established, everything is running fine and the business is paying for that.

Another way is a charge that is spread out to different parts of the business; so the IT and HR functions will all pay a chunk of money to pay for the data protection services they receive. That can help in the sense that you get a chunk of money and you don't necessarily have to worry about how each bit is being used. And if one part of the business generates a lot of subject access requests or particular issues, then in a way it doesn't matter because the cost is spread out across the organisation.

The third way, which we used when I was working at the Royal Mail's legal department, was to charge out in the same way that an external lawyer might do. We recorded our time so that the work that was done in data protection would be charged back to the different bits of the business that requested the services.

That can cause some real difficulties, because often those parts of the business don't have a budget for legal work. There would be cases where people would come for advice on a large project, and if they didn't have their budget side sorted out, it meant a lot of further administration which then deflects everybody from what they're doing. So I'm not sure that's the best way of charging for a service that is provided within an organisation. I think the difficulty with any of these things is trying to get more money and resources when you realise that you need extra help.

Probably the method of sharing data protection services as an overhead across different parts of the business makes it fairer, in that everyone sees it as a benefit that they're getting without having to foot the whole bill. It is a tricky issue for businesses, as there is probably no right way of doing it.

How do you cope with a media crisis?

Trevor Hughes: It's a combination of making sure you are doing the right things beforehand and doing the right things afterwards as well. Part of being a well-informed CPO is making sure that you are looking at the right places for information. That means making sure you are on all the privacy advocates' information lists and that you are up to speed on what the advocates and others who might be challenging you in the media are talking about.

You can stumble into a media crisis entirely inadvertently and unexpectedly. When that happens it is important to talk to the right people, and make sure you know the truth and tell the truth when you speak. For example, Doubleclick, when they announced the merger with Abacus [in 1999], they had not actually merged any offline and online data yet. Their president suggested they would, but they had not done it yet. Well, that created the Doubleclick media story and they still bear the repercussions of that. It would have been great if they had been able to get the message out right from the start that nothing had happened yet, and that it was just something that might happen.

So, a CPO should know and track the right sources, and if something does happen, know the truth, and make sure that you understand exactly what is happening within your organisation.

"Show the downside and risk potential, and make sure business units comply. But if you can, you also show the upside potential: privacy as polish on your brand, how it can help you improve customer relationships."

Trevor Hughes, International Association of Privacy Professionals