iapp

GETTING TO THE ROI OF PRIVACY

Emily Leach, CIPP/US
IAPP

Many privacy pros struggle to show their value to an organization. When advocating for more staff or budget, they are frequently asked to demonstrate what the return will be on that investment in privacy. But calculating the ROI for preventing something bad from happening is a bit like trying to pin down a cloud.

Unfortunately, that's not an answer that sits well with the people approving your budget, and you end up conflating yourself with infosecurity along the way. The good news is that there are a lot of other factors to consider than just breach prevention and response (though that's important, too). Using privacy to secure brand trust, contribute to the bottom line and gain competitive advantage, even get funding – a few years back these may have seemed like quaint ideas, but with changing consumer perceptions, privacy is now a real driver.

Here are some persuasive reasons a solid privacy program is worth paying for.

1. CONSUMERS ACTUALLY WILL CROSS THE STREET FOR A LITTLE PRIVACY

The consumer confidence index gauges consumer emotions in order to predict the performance of economic markets—it's a way of putting a number on something that's essentially not quantifiable: emotion. If consumers are feeling good about their economic outlook, says the index, they'll spend more money and improve the economy. Here's some research saying that if consumers trust you, they're more apt to spend that money with you.

According to a 2015 Forrester study, consumers are "more willing than ever to walk away from your business if you fail to protect their data and privacy." Not only that, but we're not talking about the old folks – this extends down to the 12-17-year-old group, of whom 51 percent claimed to be "very concerned about their privacy." Plus, the Forrester data shows consumers are employing tracking blockers and other technology to protect themselves more than ever.

Pew Research Center's 2014 Public Privacy Perceptions study had similar findings; 61 percent of consumers said they "would like to do more" to protect their online privacy, but many think trying to maintain anonymity online is a futile endeavor. In a 2015 study, focus groups showed that consumers are paying attention to the data-for-services (or -discounts) transaction and there are nuances in how they feel about it. One thing is for sure, they're frustrated by the lack of control they have over their data – whether how its used and who accesses it or just that the so-called targeted ads aren't well targeted.

A 2014 National Cyber Security Alliance survey, 83 percent of consumers protect their privacy by "only utiliz[ing] websites/vendors that I trust." It's easy to argue that a mature, sophisticated privacy program is going to appeal to those 83 percent of consumers.

Does your company have an app?

Taken together, 57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons.

Do you sell goods or offer services online?

Privacy protection and fraud prevention are the top non-product-related influencers in consumers' likelihood to shop with a retailer:

- Protecting personal information: 74 percent.
- Track record on fraud preventions: 54 percent.
- Commitment to corporate or social responsibility: 31 percent.

> The average company, globally, spends $1.7 MILLION on privacy — or roughly $354 per employee.
>
> —2016 IAPP-EY Privacy Governance Survey

Further, a Deloitte University Press study shows, "There is a clear connection between consumers' perceptions of data privacy and security practices and commercial success."

- Half of the consumers the Deloitte surveyed "definitely consider" the privacy and security of their personal information when choosing an online retailer
- Eighty percent say they are more likely to purchase from consumer product companies that they believe protect their personal information

The study also notes, "These findings suggest that consumer product companies have yet to establish a name for themselves as trusted stewards of consumer data — and that a company in the industry that can do so can set itself apart from the competition."

2. EVERYBODY ELSE IS DOING IT.

Okay, maybe not everybody, but some very large and very successful business are making very public moves to protect consumer privacy. Apple famously took a stand against the FBI in refusing to unlock the phone of a terrorist, citing the implications that would have for its customers' privacy. Microsoft continues to fight a months-long battle to keep private the contents of an email account held on a server in Ireland. Even the U.S. government has rolled back surveillance powers under the PATRIOT Act in response to privacy concerns.

A recent study by the IAPP and TRUSTe found that 50 percent of companies have, over the past two years, increased the involvement of privacy professionals on their information security teams to enhance the prevention of data breaches.

The most recent IAPP-EY Privacy Governance Report found the average company, globally, spends $1.7 million on privacy — or roughly $354 per employee.

Executives from the global product strategy and design firm, frog, write for Harvard Business Review about their study comparing consumer attitudes and awareness from 2011 to those in 2014. The study found that "forward-looking companies that are designing data privacy and security considerations into product development from the start, have tremendous competitive advantage and typically follow three principles – consumer education of how data is used, giving consumers control of their own data and delivering in-kind value."

Assess where your privacy program is by using a maturity model like this one, and see where you lie on the spectrum. According to that same Governance Report, mature privacy programs are more deeply involved with all aspects of the organization, leading to more budget, staff and influence.

3. KNOWLEDGE IS POWER—AND A BUSINESS ASSET

You've heard the clichés: We now live in the "data-driven economy," so we need to treat "data as currency," because "data is the new oil." But does your company act that way?

Surely, you put locks on doors, install security cameras, employ RFID tags, buy insurance and your profits probably aren't hiding under a mattress. But, most importantly, you hire people to make good decisions about how your assets are handled.

Does your company do the same for data?

In a 2010 study by Andrew Daughety and Jennifer Reinganum, the authors found that "If information is power, control over personal information affects the balance of economic power among parties;" i.e., the more control over and knowledge about the data your company holds, the more leverage you have.

Digital storage company Western Digital conducted a study in 2015 in the U.K. finding that individuals value their data at £3,241, men (£4,174) slightly more than women (£3,109). There are even a couple of companies that give customers the ability to control and sell their data as they choose.

It seems everyone agrees that data is an economic asset. Surely, it should be important to the decision makers in your organization that you have the most accurate data possible, you're keeping that data safe and sound, and you know and control who's looking at it.

Enter the privacy team. It's likely that most of your employees handle data, which means they can also mishandle data – meaning training is a must. Who's going to do that? The privacy team. You're probably going to want to implement new technology at some point. Who's going to determine how that technology affects your data assets? The privacy team.

A successful privacy team can help your company leverage its data while complying with applicable laws and maintaining customer trust. And having a privacy pro in the room when making decisions about your data is important to keeping it safe and within your control, while at the same time using it to benefit the company—and frequently the consumer, too.

4. AVOID FINES AND SANCTIONS

U.S. Federal Trade Commissioner Maureen Ohlhausen made it clear at last year's RSA conference, the FTC isn't out to get the good guys trying to do the right thing.

> "Around the globe, regulators have made it clear: They AREN'T OUT TO GET companies working to do the right things with data."

Singapore Personal Data Protection Commission member Aileen Chia told attendees of the IAPP's 2014 IAPP Asia Privacy Forum, "With our enforcement actions, we will consider what steps were taken beforehand, how cooperative the organization is and the size of the breach."

Former U.K. Information Commissioner Christopher

Graham said at the 2013 DPAs conference, "I lead an organization that wants to be effective in tackling the bad actors rather than filling out forms for people who are probably perfectly compliant anyway."

Around the globe, regulators have made it clear: They aren't out to get companies working to do the right things with data. Having a privacy team focused on protecting data, complying with laws and being transparent about ways they use data shows regulators you're one of the good guys.

5. FUNDING

Venture Capitalists are paying attention. Steve Herrod of VC firm General Catalyst told The Privacy Advisor that it's part of their due diligence, especially when companies are storing customer data, like cloud services: "What are they doing with data retention and protection?" Not only are VCs asking privacy questions at an early stage in the conversation, they're also looking for privacy-enhancing startups to invest in.

Whether you're at a start-up looking to grow quickly, or a growing company looking for funding to get to the next level, lacking a plan for privacy can be a major barrier. On the flip side, having a robust privacy team might be just the thing that gets investors to finally pull the trigger.

6. DATA BREACHES COST A LOT. AND THEY'RE LARGELY PREVENTABLE.

Okay, let's talk breach. There are lots of unknowns in the world of data breaches: When one will happen, how vulnerable you are, how much it will cost you, etc. But most people would say, *whether* one will happen is not one of those unknowns. It'll happen.

Here are a few more things we know that you can take to the bank—or at least to your CEO:

According to the 2016 Ponemon Cost of a Data Breach Study, the average consolidated total cost of a data breach increased to $4 million, and the average cost for each lost or stolen record containing sensitive and confidential information is $158, up from $154 in 2015. And a Juniper Research report has the consolidated cost of breaches at $2.1 trillion by 2019 — 2.2 percent of the estimated global GPD.

> "The BIGGEST FINANCIAL CONSEQUENCE to organizations that experienced a data breach is lost business."
>
> —Larry Ponemon, The Ponemon Institute

The Verizon Data Breach Investigation Report 2015 found that errors by employees (system administrators in particular) were responsible for 60 percent of breaches. Ponemon's study puts the number at 25 percent. That's a big discrepancy, but either way it means a lot of breaches can be stopped with some good training in handling data.

In fact, the Ponemon study found that companies can save $9 per capita on the cost of a breach by implementing employee training, and $16 with an incident response team. What do you need to implement both of those cost-saving measures? You guessed it: A privacy team.

While protecting consumer privacy is becoming more of a focus for organizations, oftentimes fallout from data breaches just doesn't seem that bad. Sales may dip for a bit, stock prices may lag for a couple of weeks, but they come around. These aren't the only factors to weigh, however. Litigation costs, new security investments, brand damage and future insurance costs are also significant business expenses.

Want to see how much a breach would cost your organization? Try one of these breach cost calculators.

The Ponemon Institute has been conducting this study for 11 years now, and founder Larry Ponemon shared some things he's learned with Security Intelligence. Among other things, he writes, "The biggest financial consequence to organizations that experienced a data breach is lost business. Following a breach, enterprises need to take steps to retain customers' trust to reduce the long-term financial impact." Ponemon also notes, "Improvements in data governance initiatives will reduce the cost of data breach."

Those aren't matters for the infosecurity team. Those are matters for a sophisticated privacy team.