Calculating the ROI for Privacy and Security

Brendan Seaton

Associate Editor, HIM&CC, President of ITAC Health and Chief Creative Officer for Privacy Horizon Inc.

One of the biggest challenges for people in health care who are responsible for privacy and security is building the business case for investment. Why would Boards of Directors and executives spend limited resources on privacy and security when there are so many competing priorities facing the organization? It's often considered crass to express privacy and security in terms of dollars and cents, but it's necessary for privacy and security officers to demonstrate a return on investment (ROI) for their programs.

ROI differs depending on whether you are in the public or private sectors. In the public sector, ROI often focusses on cost avoidance. How do we avoid the cost of a privacy breach, an investigation by the privacy commissioner, or damages in a class action lawsuit? In the private sector cost avoidance is an issue, but other, more positive factors also come into play. Maybe privacy and security are features that customers are willing to pay for. Perhaps privacy and security can provide a competitive advantage.

Determine the Investment Required

How much should an organization "invest" in a privacy and security management program? The answer to this question is going to vary depending on the size and complexity of the organization. There is a lot of guidance available as to what constitutes a comprehensive privacy and/or security management program. For privacy look to the CSA Model Code for the Protection of Personal Information. For security, ISO/IEC27002:2013 – Code of Practice for Information Security Controls is the definitive guide.

Some of the factors to be considered in the ROI analysis will include:

Staff – What is the cost of a privacy officer, a security officer and support staff?

Program development – what will it cost to develop policies and procedures, business continuity plans, incident management protocols, training and other management tools.

Risk assessment – What will it cost to assess and manage risk? Do you need a Privacy Impact Assessment and a Threat and Risk Assessment?

Program management – What will it cost to manage the day-to-day activities such as monitoring and audit, training, complaint handling and access requests?

Technical safeguards - What will it cost to implement technical safeguards such as firewalls, intrusion detection, encryption and audit logging?

Calculating the Return – Cost Avoidance

No matter how you cut it, privacy breaches are expensive. A 2016 report by the Ponemon Institute estimated that the average cost for each lost or stolen record was $158 USD. If you lose 10,000 records, that could cost more than $1.5 million. Consider the costs of losing your IT infrastructure. Even if there is no privacy breach, the loss of critical information systems to denial of service or ransomware attacks can be devastating,

Among the costs to be avoided by having an effective privacy and security program are:

Fines and sanctions – While still rare in Canada, we're seeing a steady increase in fines and sanctions imposed by regulators in the United States. It's only a matter of time before our Privacy Commissioners and courts do likewise.

Lawsuits and damages – Class-action lawsuits in response to privacy breaches are on the rise in Canada. In addition to awards for damages, the legal costs of defending the organization can be formidable.

Notification – Most privacy legislation requires that all affected individuals be notified of any breach of their personal health information. This includes informing individuals about the measures you are taking to mitigate any harm or risk that may exist.

Damage to Reputation – While reputational risk is an issue for most organizations, it is especially harmful to private sector organizations such as pharmacies, labs or HIT vendors who may lose business to their competition in the event of a breach.

Business interruption – The loss of a critical information system due to a security breach can result in significant costs due to lost productivity, disaster recovery and business continuity.

Calculating the Return – Revenue Generation

In the privacy and security world we tend to dwell on the negative. However, there are some real revenue generating opportunities associated with having a comprehensive privacy and security program in place. These include:

Funding – Canada Health Infoway and several provincial and territorial jurisdictions have made funding for digital health initiatives conditional on having appropriate due diligence for privacy and security.

Procurement requirement – Hospitals and health authorities are starting to require Privacy Impact Assessments and Threat and Risk Assessments as part of the procurement process, especially for new innovative solutions. Companies that meet the requirements have an advantage over those who do not.

Consumer confidence and trust – despite the fickle nature of consumers and their propensity to be somewhat cavalier in their behaviours, there is a growing body of evidence that there is a preference for products and services that protect privacy.

Privacy is gradually becoming a baseline requirement for digital health solutions. Over time, the business case will get easier to sell. However, privacy and security officers will need to keep their pencils sharp to ensure a decent return on investment for every dollar spent.