Towards a Model of Information Healthcare for Household Data Security

Ivan Flechais
Department of Computer Science
University of Oxford
OX1 3QD, Oxford, UK
ivan.flechais@cs.ox.ac.uk

1. INTRODUCTION

Privacy, Confidentiality, Integrity, Availability, Accountability (etc.) are all delicate concepts relating to properties of information. Tradeoffs are typically made to balance these concerns with business imperatives: e.g. user privacy vs advert supported services, availability protection vs costs of redundancy, or outsourcing to the cloud vs in-house control. The nature and extent of these tradeoffs involves significant knowledge, experience, and skill to ensure that appropriate concerns are represented and balanced fairly. In recognition of this, information security budgets have grown and the information security profession has matured in recent years to provide the education, tools, and workforce that companies can draw from. And while efforts are made to study and protect organisational settings, there remains a very significant gap in the skills, expertise, knowledge, and resources available to home users and families, and despite some initial work in exploring this domain [1][2][3] more is needed. We explore the nature of the problem of securing the home user and propose an approach modelled on healthcare.

2. HOME CONTEXT

Connected homes now generally consist of a family of multiple users accessing a number of shared and personal services through a number of shared and personal networked devices. The degree of ownership and responsibility for security for each of these devices and services varies between manufacturer, service provider, operator, and family member (e.g. routers, set-top boxes, mobile phones, social media services, media subscriptions, and online banking all have different structures of security responsibility). So too does the extent and nature of the security options and interactions available to home users (e.g. ranging from detailed configuration of networking options in routers, to no control over the configuration of set-top boxes). While some services and devices are provided with robust security "baked-in", the emergent behaviour arising from their combination can itself create security or privacy problems (e.g. account chaining, where reset information for one service is sent to another, allowing an attacker to compromise other services). It is the management of all these devices and services, in both shared and individual use, that lies at the heart of the security challenge for home users. And with the advent of the Internet of Things, the number of devices and services being made available to home users will only increase – but the time, knowledge, and budget that typical home users will allocate to securing their information is likely to remain constant. And small.

Another consideration is that the variety of different users in the home is extremely broad, consisting of one or many: children, teenagers, parents, working and non-working professionals, retired, elderly, infirm, and disabled individuals, each with a different range of education, ability, and personal interests. This is a significantly more heterogeneous group of users than most organisations have to worry about, and exacerbates the problem of designing suitable and appropriate security processes, tools, and educational material.

Catering to the needs of such a diverse population, on a topic as delicate as information security is critical to achieving the benefits of an information age, without unduly harming its beneficiaries. But while this is a challenging problem as outlined above, there are other similar ones from which to learn from. Our view is that managing information security is much the same kind of problem as that of managing health. Basic hygiene rules help ensure that information remains secure in the first place; first aid treatment is needed in the case of an incident; and advanced skills need to be deployed when facing a more complex crisis.

3. INFORMATION HEALTHCARE

Attack vectors have been compared to biological threats before (e.g. in the naming of the computer virus, or in studying the epidemiology of the propagation of internet worms). A number of attacks exist that are perpetrated by exploiting the insecurity of a small proportion of the home user population (e.g. home routers being compromised in order to DDoS online services). Securing this small proportion of users benefits others too: by securing this population, the benefits apply to all by reducing the number of possible attacks – much in the same way vaccinations help through herd immunity. But examining threats is not the only aspect of information security that has a similarity to healthcare.

3.1 Economics

The economic perspective is also compelling: many home users simply do not have the knowledge, time, or budget to devote to securing all their information even to a most basic level. In healthcare cost is also an issue, however there are a number of economic tools to make costs manageable to families – ranging from a variety of insurance policies, cooperative societies, charities, and nationally subsidised services.

Likewise, the healthcare profession has a number of services available to suit a breadth of different needs and a variety of financial constraints (family doctors, walk-in clinics, emergency medicine, specialists, etc.). While many analogous security services exist for governments and enterprises

to draw from, there are very few counterparts in the information security of homes and families, which is and remains remarkably ad hoc and informal.

3.2 Awareness, Education, and Training

While the importance of information security for home users is nowhere near as obvious or visceral as that of healthcare, it is nonetheless crucial to prosperity in an information-centric context. It is therefore disappointing that the resources devoted and available to home users tend towards the perfunctory and overly simplistic: security awareness campaigns, exhortations to install patches, injunctions against choosing bad passwords, etc. The focus is on getting home users to be more aware, however the problem does not go away once users are aware: there needs to be also an understanding of the nature of the problem and its solutions.

The healthcare sector runs awareness campaigns to communicate about health issues, and frequently targets specific population demographics according to their risk of contracting specific diseases – however this is only one part of an infrastructure which ultimately aims to prevent, diagnose, and treat illness. Campaigns are complemented by options for personalised advice, investigation of symptoms, and treatment of problems. Supporting this are educational and training opportunities that provide up-to-date knowledge and skills to suit the different roles within this infrastructure (e.g. doctors, nurses, technicians, first responders, pharmacists, etc.). Taken as a whole, this is a comprehensive, evidence-based approach to preventing, detecting, and reacting to threats to the health of a population.

3.3 Infrastructure

The information security infrastructure has largely evolved out of the need for protecting government, critical national infrastructure, and banks; and training and education about information security has targeted these. As a result the tools, policies, processes, and financing of information security services are geared towards larger organisations, that have the manpower and resources to devote to procuring them. But those in need of information security are growing and more diverse than ever: "in 2013, 74.4 percent of [U.S.] households reported Internet use" [4]. And more than homes: home offices, small, and medium enterprises all need more tailored security services, tools, and education.

Information healthcare requires an infrastructure to enable homes and families to cope with the growing complexity of the information age. The alternative is that we will continue in the current ad hoc manner, where only large organisations and a select few others have the knowledge, expertise, and resources to protect themselves, and where everybody is more at risk from the insecurity of others.

4. RESEARCH DIRECTIONS

In healthcare, *primary care* relates to the work of health professionals who act as a first point of contact. For more specific needs, *secondary* and *tertiary* care refer to services that provide advanced care. *Public health* focuses on threats to populations, and its methods aim to detect, prevent and treat threats on a much broader basis (see Figure 1).

There are clear distinctions between public health and patient-focussed approaches, but the key is that they operate in concert with one another.

Drawing from this, we need to explore a combination

	Public Health	Primary Care	Secondary/Tertiary Care
Roles	Epidemiologists, biostatisticians, environmental health officers, pharmacists, veterinarians, …	GPs, nurses, pharmacists, …	Consultant specialists & surgeons, Acute care staff, Occupational therapists, …
Services	Disease control (e.g. vaccination), Education & Training in healthy behaviour, Early warning system for public health emergencies, Investigate health hazards	Preventive care, Management of chronic conditions, Health education, Initial consultation for new concerns	Acute care, Specialist diagnosis & treatment
Characteristics	• Population-centered • Equitable • Proactive • Health promoting • Risk reducing • Effective • Efficient[1]	• Person-centered • Comprehensive and integrated • Continuity of care • Participation of patients, families and communities[2]	• Person-centered • Complex • Specialised • Institution-based • Relatively uncommon[3]

[1]http://www.hhs.gov/ash/initiatives/quality/
[2]http://www.who.int/whr/2008/whr08_en.pdf
[3]http://www.hindawi.com/journals/scientifica/2012/432892/

Figure 1: Roles and characteristics of healthcare

of "public health" and "patient-focussed" approaches that complement one another to protect household data. We also need to explore the concepts of primary and secondary *data care* services for housholds, continuity of care (to foster trust), and investigate participation opportunities from families, and communities.

With regards to future research, we note that:

- household security education requires both population- and person-centric approaches;
- continuity of care can help foster trust in data security;
- information healthcare for households is multidisciplinary – key roles need to be defined for this infrastructure;
- the nature and extent of harm to (and from) households from data security breaches needs exploring.

5. CONCLUSION

We have argued that information security is a problem that has a number of analogies to healthcare and highlighted that the current infrastructure of information security is not well suited to the problems of smaller organisations – particularly those of the home. We propose the concept of *information healthcare* as a model of the research necessary to understand the specific needs of providing security to homes, and argue that the economics, education and training, and infrastructure of healthcare are important starting points.

6. REFERENCES

[1] C. L. Anderson and R. Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, 34(3):613–643, 2010.

[2] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 209–223. IEEE, 2012.

[3] Y. Li and M. T. Siponen. A call for research on home users' information security behaviour. In *PACIS*, page 112, 2011.

[4] U.S. Department of Commerce, Economics and Statistics Administration. Computer and internet use in the united states: 2013. `http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf`.