SUBMISSION No. 71

Submission to Australian Parliamentary Inquiry into Cyber-Safety

Overview

The System Administrators Guild of Australia (SAGE-AU) is Australia's premier professional organisation dedicated to the support of the profession of system administration. Systems administrators work in all varieties of profit and not-for-profit industry, education, research and government, in roles spanning from junior administrators to chief information officers. SAGE-AU has membership to the Internet Industry Association (IIA) and to Professions Australia.

In this submission, SAGE-AU provides commentary on the following elements pertinent to the terms of reference:

- The online environment in which Australian children currently engage
- The nature, prevalence, implications of, and level of risk associated with online threats
- Australian and international responses to current threats, their effectiveness, and costs to stakeholders including businesses
- Opportunities for cooperation across stakeholders
- Opportunities presented by new technologies, and the economic benefits thereof
- Information on best practices in protection

As an organisation, SAGE-AU firmly believes in appropriate protection for all Internet users in Australia. In general, this can be summarised as follows:

- Education in Internet-appropriate behaviours for all Internet users, especially children;
- Technological measures applied on end user computers, as and where required, including but not limited to appropriate anti-virus protection, firewalling, application of appropriate software updates, and local filtering as deemed appropriate by equipment owners; and
- Use of law enforcement to deal with illegal material, content, or criminal behaviour in a timely and effective fashion.

SAGE-AU's spokesperson on this matter is Ms Donna Ashelford. The organisation can be contacted via any of the following means:

- Email info@sage-au.org.au
- Post SAGE-AU, Industry House, 375 Wickham Terrace, Brisbane QLD 4000
- Phone 07 3842 2235

The Internet's Current Landscape: an Australian perspective

As a professional organisation made up of the individuals who make the "`net work," SAGE-AU has a unique and deep understanding of the Internet in the Australian context. The Internet is one of the most broadly used business and personal tools, with many forms of commerce now depending on it in large part, or for some organisations, exclusively. The impact due to outages and other issues is therefore widely felt by the community. SAGE-AU's membership is in large part responsible for ensuring that this infrastructure remains running, and therefore has a professional and ethical obligation to understand the technology as fully as possible.

According to the Australian Bureau of Statistics (ABS, 2010) there were over nine million business and personal subscribers to Internet services as at December, 2009. In 2009, the ABS found that 72% of Australian households had home Internet access (ABS, 2009).

The ABS also found (ABS, 2009) that 79% of Australian children aged 5 to 14 years used the Internet, with home (73%) being a more common site of Internet usage than school (69%). It is therefore apparent that the primary influences on a child's Internet access and usage are caregivers and educators; to this end, SAGE-AU supports measures designed to empower these stakeholders in the appropriate protection of children in the online environment as elsewhere. SAGE-AU believes that appropriate protection can be defined as follows:

Appropriate education for all Internet users. The Internet differs from most preceding technologies in its reach, in its flexibility and adaptability, in the pace of its evolution, and its modes of use. This makes education in how to use it, and specifically how to do so appropriately, of utmost importance. The same lessons that apply in the physical world apply on the Internet, and for the same reasons. In many cases, a simple reapplication of these real world lessons will work effectively; for example, there exists no reason that campaigns similar to the offline "Stranger Danger" campaign would not work in the Internet context.

To the layperson, the Internet is not a well-understood or defined medium; it is simultaneously similar to, yet different from, all previous forms of communication. In some ways it resembles a broadcast medium equivalent to radio or television, allowing content producers to access a broad range of consumers with relative ease. However it also shares properties with point-to-point communications technologies, allowing individuals to communicate in relative privacy. Legislators worldwide have on various occasions attempted to attribute these properties to the Internet, with varying degrees of success. Moreover, the Internet is no one technology; it is a rapidly evolving suite of technologies, increasing the risk that legislation *and* technological solutions to real or perceived problems are outmoded prior to effective deployment. While the Internet is a very complex tool – the most complex ever developed – it, generally speaking, needs no more special legislative treatment than analogues in the offline context.

Technological measures on end user systems. The rate of evolution associated with the Internet makes any centrally deployed protection mechanism of any type, no matter how conceived, less than effective. No sooner than a system of this nature is deployed, it will be circumvented and/or rendered useless by local or international users, by changes in the communications protocols used on the Internet, or by a simple use of cryptographic systems. Indeed, several web browsers – Opera for example (Opera, n.d.) – come pre-built with suitable circumvention technology, making the approach moot.

Furthermore, centrally deployed systems are – by their nature – inertia-prone and subsequently slow to adapt. To this end, SAGE-AU recommends all end user systems utilise an appropriate mix of technological protection measures, including but not limited to regularly updated anti-virus software, local network firewalling, and software updates as and when provided by vendors. Caregivers should continue to have the ability to install appropriate Internet filtering software as and when they deem necessary on each end user system; this is a tool that should also be available to public use terminals as and where appropriate.

However, no amount of technological protection compensates for appropriate education. New viruses and worms can circumvent anti-virus software, defy firewalls, and exploit unpatched defects in software; no Internet filtering tool to date deals with every possible use of the Internet. Caregivers should, therefore, consider whether it is appropriate for children below a certain age to have access to a computer in the privacy of their own bedroom, or whether that computer should instead be located in a more open setting in the home.

Active policing by state and federal law enforcement. Just as the "real world" consists of a range of individuals and groups of varying moral fibre, so does the Internet; international organised crime has found the Internet to be a lucrative playing field, with bank fraud (in the form of so-called "phishing" scams) one of the most common. In general – and save for physical crimes against the person – if a particular element of illegal behaviour can be found offline, it has an analogue online. With this in mind, a properly funded, well resourced, and technically savvy police presence is recommended by SAGE-AU. In turn, this should foster relationships both with international police forces, with Internet Service Providers (ISPs) and major content producers, and with professional groups.

In particular, it is SAGE-AU's view that Internet professionals, ISPs, and content producers have a responsibility to work with law enforcement in ensuring that illegal behaviour is dealt with appropriately and rapidly.

The Threat Landscape

The ABS (2009) found that only three percent of children had a reported safety or security problem while using the Internet. While any number of personal security issues involving children is cause for concern, it is SAGE-AU's belief that this figure is reflected within the wider community both online and offline. To this end, SAGE-AU does not believe the Internet poses any greater or lesser threat to any member of the community – including its children – than any prior technology or social development.

The kinds of threats for which the Internet is known generally mirror those found offline. The most commonly known threats include malware (malicious software), SPAM (unsolicited communications, typically of a commercial nature), and financial fraud; organised crime syndicates and more enterprising sole criminals often use one or more of these at a time in undertaking their activities. While technological fixes – anti-virus, anti-spam, and multi-factor security – exist to address these issues, in every case education of content users, content producers, and law enforcement provide the most effective long term results.

Bullying, Stalking, and Sexual Grooming

In recent years, much has been made of the apparent use of the Internet in compromising individuals' personal safety; in particular, the use of the Internet in "cyber bullying," "cyber stalking," and/or the sexual grooming of individuals, particularly children. While these threats are real and have been detected occurring, they have immediate analogues offline, as evidenced by the titles ascribed to them, and indeed the same approaches should be taken to dealing with these problems online as offline.

Again, education is the first and best defence, and SAGE-AU recommends an online analogue of the "stranger danger" campaign; ensuring that children know with whom it is safe and appropriate to converse is as important on the Internet as it is in the street. SAGE-AU recommends that parents and teachers be given the education, tools, and support needed to understand the programs and sites frequented by children, in effect to become as "netwise" as they are "streetwise." In place of discouraging educators to use commonly accessed websites such as Facebook (Facebook, n.d.), SAGE-AU believes that schools and education departments should instead be encouraging judicious use and familiarisation of these tools, and of any tools which from time to time come to replace those currently in use.

Inadvertent Access to Age-Inappropriate or Illegal Material

The issue of "inadvertent" access to age-inappropriate or illegal content has become something of a political red flag of late, with all manner of interest groups (including SAGE-AU) expressing an opinion on this matter. Given the size and scope of the Internet, it is certainly not implausible that individuals can from time to time be inadvertently exposed to unsavoury material; equally, SAGE-AU is aware of vanishingly few cases where this has occurred. Suitably concerned caregivers continue to have the option of installing Internet filtering software to mitigate this risk, but should also be aware that this is by no means a substitute for appropriate supervision.

SAGE-AU's position on centrally administered (ISP-level) Internet filtering as a means to address this issue has been well communicated. In summary, SAGE-AU believes that ISP level filtering is: an ineffective use of taxpayer and business funds, with a limited scope for success; subject to negative performance implications particularly for high traffic websites and ISPs; prone to "scope creep" under future administrations; and insufficiently subject to judicial or community overview. Moreover, a substantial portion of Internet traffic – and much of the Internet's illegal material – is now carried over communication protocols including BitTorrent, protocols which are not subject to filtering by ISP-level Internet filtering, rendering the filter ineffective at dealing with the deliberate trade in illegal material. SAGE-AU instead recommends focusing resources on user education, law enforcement, and software and services for individual end user systems.

Inappropriate Social and/or Health Behaviours in the Online Environment

The Internet's nature makes it very easy for like-minded individuals to find each other and form interest groups on almost any topic, including those not generally deemed socially or morally acceptable; this does from time to time raise community concerns as to the impact of this suite of technologies. Given the nature of the Internet and its flexibility, this is an area where no broadly effective technological prevention technique exists: for example, any conceived technical filter for online conversations including any given word or phrase is likely to not only block material of community concern, but will also block the majority of material on the subject, whether unsavoury or not. Simply blocking based on a list of web sites or other identifiers is an unsustainable solution, based both on the amount of existing material available on the Internet and on the rate of creation of new material.

As pertains to children's use of the Internet, supervision of Internet use is a key mitigation in ensuring that their access to inappropriate material is limited.

Identity Theft and Breaches of Privacy

The Internet allows criminals and criminal groups many means by which to steal personal data; this may in many cases be used to create an identity by which further crimes may be conducted. This can range from the relatively simple theft of a user's credit card details, subsequently using those details to fund purchases, through to the acquisition and reuse of substantial identifying information with the intent of perpetrating much broader frauds. The methods of acquisition of data are varied, and include specially crafted malicious software, fraudulent websites designed to resemble those of legitimate organisations, unsolicited emails promising riches in return for various forms of assistance, theft of corporate databases, and so on. Some of these have suitable technical mitigations; malware can for example be addressed by the use of anti-virus tools.

Again, user education in conjunction with clearly defined industry codes of practice remains the most effective long-term solution to these problems. For example, ensuring that users well understand that they will never receive an email from their financial institution asking for their password, and also ensuring that financial institutions never send emails asking for such details, limit the scope and effectiveness of the fraud known in the Internet industry as "phishing."

To date, Australia does not have a clearly defined code of practice covering any area of electronic commerce or banking; nor does it have legislation requiring mandatory disclosure of compromises or suspected compromises involving information systems that contain or may contain user-identifying data. In this regard, Australia lags behind other world leaders; it is SAGE-AU's view that this is an area in need of improvement.

Australian and International Responses to Current Threats

As a relatively nascent environment, there exists no coordinated or well-defined response mechanism to deal with threats on the Internet, within Australia or internationally; in general, the mechanisms by which threats are addressed are still ad hoc and vary from organisation to organisation. Some entire industries have a better response mechanism than others, with the financial services industry being well versed in dealing with threats, and having formed a process by which to deal with these that generally works. The notion of a national Computer Emergency Response Team (CERT), supporting law enforcement, industry, and professionals' groups, and in conjunction with clearly defined threat response processes, is viewed as important by SAGE-AU.

Given the ad hoc nature of the response to threats, no completely clear picture exists of the cost or impact to stakeholders. Various Internet security companies, including Symantec (n.d.) and Cisco (n.d.) from time to time publish trend reports, which can be used to extrapolate as to the costs of a limited suite of threats to all business, but few such reports exist covering the costs to non-commercial entities. It is however clear that these threats have a real cost, with 75% of surveyed organisations experiencing an online attack of some type in 2009 (Symantec, n.d.), with one group suggesting that an average cost per data breach was US$204 per exposed user record (Moscaritolo, n.d.).

Opportunities for Cooperation

Australia is in an excellent position to become a leader in this space. With no pre-defined international guidelines of note, Australia can begin to set industry standards for appropriate cooperation between government, law enforcement, ISPs, users, and technical staff, both within Australia and to overseas organisations. As the leading organisation providing support to system administrators, SAGE-AU is willing and able to provide guidance in the best ways to achieve cooperation.

With this in mind, SAGE-AU recommends a documented industry code of practice to encourage inter-organisation cooperation, backed by mandatory disclosure legislation for matters pertaining to security of end users' data. SAGE-AU also recommends well-funded and resourced law enforcement, with the technical capability to act on information communicated to them by stakeholders.

Seizing and Maximising the Use of New Technologies

As the system administrators responsible for Internet systems, SAGE-AU firmly believes that new technologies can have their place in technical solutions to specific identified problems. The Internet is a rapidly evolving suite of tools and technologies, and with this in mind, the tools and technologies used in support of the Internet need to evolve equally rapidly. SAGE-AU's membership are well placed to assist in the evaluation of new technologies and tools as and when they become available – and indeed do in the course of their professional duties. The SAGE-AU code of ethics requires that members maintain knowledge of current tools, technologies, and skills.

It is important however to note that SAGE-AU does not believe that every problem has a technical solution; problems of a primarily social nature should be addressed through education and policing before being addressed technically, as this minimises the risk of "collateral damage," through ill conceived technical solutions inadvertently impacting upon legitimate, socially accepted service use. Generally, the most appropriate place for protection tools is as close as possible to the end user – ultimately, the end user system.

Achieving and Maintaining World Best Practice Safeguards

There are already codes of practice in place and in use within individual industries, and the National Privacy Principles provide a good basis from which organisations can and should work when dealing with users' data of any type. SAGE-AU believes that other perceived risks, including risks to individuals including children, are most appropriately dealt with through education and policing.

With this in mind, SAGE-AU recommends a documented industry code of practice to encourage inter-organisation cooperation on education and reporting to law enforcement, backed by mandatory disclosure legislation for matters pertaining to security of end users' data. A suite of recommended client side protection tools, and appropriate methods for advising users of their options in this regard, would be a highly appropriate component of this code of practice.

Online Ombudsman

SAGE-AU applauds the concept of an independent online ombudsman. As in the telecommunications industry, the ombudsman's primary responsibility should be in advocating for users and other stakeholders and in resolving user concerns. Further, SAGE-AU believes that the ombudsman's responsibility should be to advocate to government and law enforcement, and within Internet centric industries, on matters pertaining to Internet usage education and policing.

Conclusions

In providing the above information, SAGE-AU's main goal is to foster discussion and an environment of cooperation with government, law enforcement, industry, and other interested users groups in shaping the Australian Internet landscape. While it believes that the relative 'threat' posed by the Internet to individuals including children is no higher than that found elsewhere in society, SAGE-AU firmly believes in the judicious use of a range of tools in dealing with both perceived and real Internet threats. This includes but is not limited to the use of end user education, effectively resourced law enforcement, and appropriate technological measures used in appropriate ways, particularly on end user computers.

While SAGE-AU's members are the individuals who support, operate and maintain Internet infrastructure within Australia, the organisation is very conscious of technology's place in dealing with social issues, and believes that the Internet does not in and of itself require legislators to approach existing social issues in novel ways. Finally, SAGE-AU is ready and willing to engage with government, legislators, law enforcement, and industry groups to better foster cooperation in managing the Internet in ways appropriate to Australian conditions.

Statement of Authorisation and Contact Details

Submitted on behalf of the System Administrators Guild of Australia (SAGE-AU), Industry House, 375 Wickham Terrace, Brisbane QLD 4000, telephone 07 3842 2235.

Authorised by Ms Donna Ashelford, Corinda, in her capacity as SAGE-AU's president. Ms Ashelford is contactable on email at president@sage-au.org.au .

References

Australian Bureau of Statistics. (2009). Household Use of Information Technology, Australia, 2008-09. Retrieved from http://abs.gov.au/ausstats/abs@.nsf/mf/8146.0/ on 10 June, 2010.

Australian Bureau of Statistics. (2010). Internet Activity, Australia, Dec 2009. Retrieved from http://abs.gov.au/ausstats/abs@.nsf/mf/8153.0/ on 10 June, 2010.

Cisco Systems. (2008). 2008 Internet Security Trends: A Report on Emerging Attack Platforms for Spam, Viruses and Malware. Retrieved from http://pages.ironport.com/trendsreport2008.html on 11 June, 2010.

Facebook. (n.d.). Retrieved from http://www.facebook.com/ on 10 June, 2010.

Moscaritolo, A. (2010). Data breaches cost organisations US$204 per record in 2009. Retrieved from http://www.securecomputing.net.au/News/165617,data-breaches-cost-organisations-us204-per-record-in-2009.aspx on 11 June, 2010.

Opera. (n.d.). Opera Web browser: Opera Turbo. Retrieved from http://www.opera.com/browser/turbo/ on 17 June, 2010.

Symantec Corporation. (2010, April). Symantec Global Internet Security Threat Report: Trends for 2009. Retrieved from http://www4.symantec.com/Vrt/wl?tu_id=SUKX1271711282503126202 on 11 June, 2010.