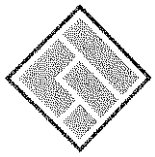
Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:5A
Received 6 May 2003

Mr Keith Inman
Director Electronic Enforcement
Australian Securities & Investments Commission
GPO Box 9827
SYDNEY NSW 2001
☎02 9911 2679 🖹02 9911 2621
E-mail:



ASIC

Australian Securities & Investments Commission

5 May 2003

Ms Maureen Weeks
Secretary – Parliamentary Joint Committee
on the Australian Crime Commission
Parliament House
Canberra ACT 2600

Dear Ms Weeks

I refer to your recent letter advising of the Committee's inquiry into trends in cybercrime techniques and practices.

The Australian Securities & Investments Commission (ASIC) has re-considered the terms of reference and is pleased to forward the attached submission.

We thank you for alerting our agency to this inquiry. ASIC would be willing to provide additional information if that would assist the Committee in its deliberations.

Yours sincerely

Keith Inman
Director Electronic Enforcement

The Australian Securities and Investments Commission (ASIC) welcomes the opportunity to comment on the Parliamentary Joint Committee's inquiry into cybercrime. In responding to the current inquiry, reference is made to ASIC's previous submission in regard to the Committee's inquiry into the impact of high technology crime on the National Crime Authority in 2001. Many of the comments made in ASIC's submission then still apply. As a result, the following comments relate to ASIC's interests in threats to the Critical Information Infrastructure (CII) an element that was not covered in our previous submission.

By way of introduction, ASIC is one of three[1] Commonwealth government bodies that regulate financial services and is the single national regulator of companies. ASIC regulates advising, selling and disclosure of financial products and services to consumers, protecting markets and consumers from manipulation, deception and unfair practices. ASIC is a law enforcement agency with investigative staff around Australia undertaking both criminal and civil actions.

In performing its functions and exercising its powers, ASIC must (in part) strive to;

- Maintain, facilitate and improve the performance of the financial system and the entities within that system in the interests of commercial certainty, reducing business costs, and the efficiency and development of the economy, and
- Promote the confident and informed participation of investors and consumers in the financial system[2].

Clearly the arrival of the e-commerce technologies have provided, and will continue to provide, benefits to the financial system and consumer protection. For instance, these technologies assist ASIC to;

- Provide consumer warnings on prevailing on-line scams,
- Provide public access for investors and consumers to information on Australia's 1.2 million registered companies and the thousands of people and entities registered to operate in our financial sector, and
- Increase the speed at which information is disclosed to the market place.

ASIC is, therefore, interested in mitigating the risk of any eventuality threatening consumer confidence in e-commerce or the accrual of benefits to the Australian financial system.

ASIC recognises, however, that the use of technology may also increase the level of attendant risk to business and consumer confidence. ASIC has reason to believe a single significant compromise or outage in a major Australian institution could undermine consumer confidence and have a serious negative impact on the reputation of financial markets.

---

[1] APRA and the RBA being the other two.

[2] ss1(2) ASIC Act 2001

Furthermore, the negative impact of a single information infrastructure catastrophe can be matched by the cumulative effect of many small impact e-crimes perpetrated over a period of time. An e-commerce sector that is plagued by cybercrime will not engender the trust and confidence of investors and consumers.

A survey[3] last year found that security scandals are keeping 45% of customers away from Internet banking. One estimate in 2001 suggested cybercrime cost companies worldwide approximately $3 trillion dollars each year[4]. The Sydney Morning Herald recently stated that the latest FBI statistics regarding Internet fraud indicates a tripling of complaints in the last year[5]. Such high cost impact estimates do have to be qualified by the paucity of empirical data. Anecdotal data does, however, support an upward trend. For instance, ASIC saw electronic enforcement requests grow from 8 per annum to more than 200 within a period of 24 months

ASIC recognises that its enforcement efforts and those of other agencies in prosecuting e-crime play an important role in shoring up consumer confidence. Consumers should expect the same level of protection in the electronic environment, as they are accustomed to in the physical environment. E-commerce technologies have, however, significantly increased the threats to markets and participants and they have also significantly increased the challenges to ASIC's enforcement operations.

As financial services/product providers and intermediaries take advantage of e-commerce technologies to interact with each other and with consumers, ASIC has had to come to terms with the implications for its enforcement activities. These comments can be placed in context by use of a case study of a typical electronic enforcement matter within ASIC.

From time to time ASIC will become aware of postings on a web site that appear to contravene the law. For instance, a series of false and misleading statements intended to induce people to buy particular stock (usually because the offender has taken a position in the shares and will benefit if the price increases or decreases). To investigate, ASIC has to track the postings back to the source. The person concerned will have operated with the belief that they were anonymous. In some instances, however, when people make postings to the Internet they leave behind electronic 'footprints' that can be tracked.

In this case ASIC was able to trace the electronic trail from the public registers of Internet domain names, through the content provider who hosted the site containing the offending postings, through the Internet service provider who provided the connection services, through a telephony carrier's infrastructure, to a company's network gateway. At that stage ASIC was able to prove that the electronic identifiers for the postings (the Internet Protocol 'IP' numbers)

---

[3] Corillian International Survey. Reported in the Australian newspaper "Security fears hurt e-banking" Karen Dearne. 5th March 2002.

[4] Insurance Council of Australia: CyberCrime and Vandalism – Defence Plan for the General Insurance Indsutry. 2001

[5] SMH. 14/4/03 http://www.smh.com.au/articles/2003/04/13/1050172476237.html

translated back to the company's Internet gateway, its firewall[6]. The company's firewall logs confirmed that its IP number had accessed the Bulletin Board site and had been used to post text to the site. The company did not, however, have the relevant logs turned on to capture which users were using what IP numbers at any particular moment in time.

With 250 employees in the company, this might have been the end of our investigation had other inquiries not revealed that a suspect worked for the company. Using search warrants, ASIC obtained a forensic examination of the suspect's office PC and within the Internet cache of the PC located copies of the offending postings.

The above case study allows for a number of environmental observations to be made concerning operational risk factors:

- The entire ICT infrastructure involved was publicly owned.
- The integrity of public registers is critical.
- The reliance upon private companies to maintain appropriate records, (particularly ISPs).

Any one of the above risk factors can jeopardise an enforcement outcome. ASIC's ability to directly control or mitigate these risks is limited and as a result it will routinely investigate matters that it cannot bring to a satisfactory outcome, because the trail simply dries up.

This is the situation facing ASIC and every other agency or regulator. It doesn't matter if you are investigating a market manipulation via an Internet bulletin board, or a denial of service attack as part of an extortion attempt, or a possible intrusion on a critical information infrastructure (CII) asset. Although motivation may differ, the risk factors apply equally. Furthermore, companies will increasingly face these issues as they embrace e-commerce and are forced to deal through the courts to settle business disputes requiring authentication of disputed communications or electronic transactions[7].

This area of commonality between government and industry infers that there are synergy opportunities in agencies working together and in governments working with industries. For instance, if a solution to national security concerns about attacks on a particular CII asset in the private sector is to harden the target (through more robust I.T. security architecture and increased redundancy), then that action also hardens the target against profit motivated crime[8] and will ensure that should a dispute arise, the company is well placed to prove the facts. Such cooperation makes additional sense because;

---

[6] A firewall is a hardware device, or software, that controls access to a particular network or network segment.

[7] See, for instance, the proof requirements associated with a Digital Certificate transaction. PKI Legal Report. NOIE. May 2002. (http://www.noie.gov.au/publications/NOIE/Authentication/PKI_legal_report_May2002.pdf)

[8] It does this in a number of ways: Firstly, it is more difficult for criminals to intrude from the outside thereby acting as a deterrent. Secondly, it ensures the infrastructure is in place to identify criminal attempts from internal sources (be that against the company itself, or against third parties). Lastly, as a crime prevention strategy it reduces the level of matters reported to law enforcement agencies to

- Environmental risk factors cannot be mitigated by a single agency (in the absence of legislative powers) or a single corporation (in the absence of industry support), and
- The magnitude of harm from either a single CII failure, or a negative e-crime trend, has the potential to effect whole markets, industries, or even economies. Such consequences make cooperation appealing.

ASIC is aware of a number of government/industry cooperative ventures, which it has recently participated in, that mitigate the aforementioned environmental risk factors:

1. Australia's Internet domain name authority (auDA) is responsible for establishing policy on the allocation of domain names in the .au space. A not-for-profit company, auDA has welcomed collective input from a range of agencies in the development of Australian domain policy. As a result, agencies believe Australia is well placed in having a public registry with a high degree of integrity, in comparison to many other jurisdictions. It is not a coincidence that the vast majority of web sites scams are sourced outside of the .au space.

2. The Internet Industry Association will shortly be releasing its Cybercrime Code of Practice. The code will provide guidance to IIA members on best practice for assisting agencies conducting e-crime and national security investigations. It will include data retention standards, as well as information sharing and evidence handling guidelines. Developed in consultation with Police Services, law enforcement agencies, national security agencies and the Commonwealth Privacy Commissioner, the code is thought to be the first such industry led example anywhere in the world.

3. Standards Australia's Committee IT/12, Information Systems, Security and Identification Technology is working with industry and agency representatives to develop guidelines for the management of I.T. evidence. This resource will provide guidance on the importance of, and techniques for, maintaining appropriate records. These guidelines will ensure companies are well placed to protect their rights and property in an electronic environment.

---

consume investigative resources. (Although there may be a counter argument that the potential crime is displaced to a 'softer' target. See e-Crime Solutions and Crime Displacement. AIC Trends & Issues No. 243).