Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:30
Received 8 September 2003

Mr Peter Coroneos
Chief Executive
Internet Industry Association
PO Box 3986
MANUKA ACT 2603
☎02 6232 6900 02 6232 6513
E-mail: peterc@iia.net.au

Internet Industry Association

N E W S R E L E A S E

For Immediate Release
Monday, 21 July 2003

IIA Releases Draft Cybercrime Code of Practice

The Internet Industry Association today released its draft Cybercrime Code of Practice for public consultation.

The Code is the product of over 18 months' development by the IIA Cybercrime taskforce. It defines the rights and responsibilities of Internet Service Providers in meeting their enforcement co-operation obligations, while preserving, to the full extent the law, the sanctity of their customers' personal information. The IIA sees the Code as forming day to day operational guidelines to enable ISPs to assist law enforcement and national security agencies in the execution of their duties.

IIA chief executive, Peter Coroneos explained that the Code aimed to address the frustrations of law enforcement agencies who have too often found that by the time they approach an ISP for information about suspects, the data has been overwritten or discarded. In other countries such as the UK, legislators have stepped in and required data retention for up to seven years.

"Our draft Code stipulates retention periods of six or 12 months in Australia, depending on the information in question. We think this is a more reasonable period than other countries have imposed, and the Australian law enforcement agencies we have consulted with evidently agree, given their support for the initiative."

Mr Coroneos emphasised the lengths the IIA had gone to in protecting the balance between privacy and cooperation with law enforcement investigations into cybercrime and cyberterrorism . "In framing the Code, we have been at pains to strike what we are convinced is a reasonable balance. Where ISPs already collect customer information in the course of their business operations, this Code stipulates minimum retention periods for that data. "

Contrary to some publicly expressed concerns, the Code does not require ISPs to capture caller line identification (CLI) or caller name display (CND) data. Instead, it says that if an ISP becomes in a position to access this data under arrangements with their telco providers - for example as an anti fraud measure - then they must retain it for 6 months. During this time a law officer with a warrant or 'section 282 notice' can request the ISP to provide this information, which can be helpful in locating criminals hiding behind the anomity of an unlisted number.

However, the Code reminds ISPs that if they disclose this information to anyone other than a law enforcement agency acting under lawful authority, they will be in breach of the Telecommunications Act and at risk of a criminal penalty and up to two years imprisonment. Further, by requiring all ISPs wanting to be party to the Code to become bound by the Privacy Act, the powers of the Privacy Commissioner can be invoked, leaving the way open for compensation and other orders.

"It is important that when dealing with sensitive issues like privacy, that we don't allow a two-tier set of compliance to arise. The same rules must apply to everyone if they are to benefit from the certainty that this Code seeks to provide.".

The public consultation period for the draft Code ends on 21 August 2003. The Code is available from www.iia.net.au/cybercrimevt.html.

Ends.

More: For more information see www.iia.net.au/cybercrime.

Peter Coroneos, Chief Executive IIA (02) 6232 6900

--

ABOUT THE IIA

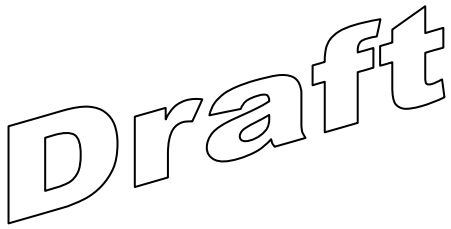
The Internet Industry Association is Australia's national Internet industry organisation. Members include telecommunications carriers; content creators and publishers; web developers; e-commerce traders and solutions providers; hardware vendors; systems integrators; banks, insurance underwriters; Internet law firms, ISPs; educational and training institutions; Internet research analysts; and a range of other businesses providing professional and technical support services. On behalf of its members, the IIA provides policy input to government and advocacy on a range of business and regulatory issues, to promote laws and initiatives which enhance access, equity, reliability and growth of the medium within Australia.

INTERNET INDUSTRY

CYBERCRIME CODE OF PRACTICE

CODES FOR INDUSTRY AND SELF REGULATION AND RULES OF ENGAGEMENT WITH LAW ENFORCEMENT AGENCIES IN RESPECT OF INVESTIGATION PROCEDURES REGARDING ONLINE FRAUD AND OTHER CRIMINAL AND TERRORIST ACTIVITY

Public Consultation Draft 2.0
July 2003



Internet Industry Association
www.iia.net.au

CONTENTS

1. BACKGROUND

1.1 The Internet Industry Association (**IIA**) and Law Enforcement Agencies (**LEAs**) recognise a commonality of interest between industry and government in prevention, detection and investigation of online fraud and other criminal activity and threats to national security and information infrastructure generally.

1.2 The internet, including email and the world wide web, continues to deliver enormous efficiency benefits to business and to facilitate free flow of information and ideas. Confidence of consumers and business in the use of information infrastructure as a means to do business and communicate is dependent upon that infrastructure being safe (for example, free from virus, denial of service and hacking attacks), secure from unwarranted intrusions upon personal privacy and commercial confidentiality, and reliable.

1.3 Safety, security and reliability of the internet is dependant upon early detection of criminal activity that might undermine achievement of these objectives. However, this requires a balancing of such fundamental rights as the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities. To address the legitimate rights and expectations of law abiding citizens to the protection of their personal information, the IIA has also drafted an Industry Code of Practice for Internet Privacy [IIA Privacy Code of Practice found at http://www.iia.net.au/privacyvt.html], and remains committed to promoting industry best practice for the privacy of those using the internet for lawful purposes.

1.4 Telecommunications law in Australia has for many years imposed obligations on telecommunications carriers and carriage service providers (CSP's) to cooperate with LEAs and facilitate interception of telephone calls in accordance with interception warrants obtained by the LEAs. The *Telecommunications (Interception) Act* was enacted in 1979 and provides the lawful basis for intercepting communications. As such the practices in place are well developed. However, the appropriate manner and procedure for cooperation between LEAs and Internet Service Providers (**ISPs**) in relation to detection and investigation of online fraud and other criminal activity and security threats has not been well understood. This Code addresses that area.

1.5 This Code builds upon other relevant codes and information sheets, referred to in section 2 of this Code to provide a basis for ongoing cooperation between LEAs and ISPs in relation to prevention, detection and investigation of online fraud and other criminal activity and threats to national security and information infrastructure.

1.6 This Code has been developed recognising the cost of online fraud and other criminal activity, and the cost of its prevention, detection and investigation. Online fraud imposes a substantial cost on ISPs that is ultimately borne by internet users. Smaller ISPs are disproportionately affected because of the more limited resources available to them to limit their exposure and secure their networks. Denial of service, hacking and other security threats and attacks impose high costs on business using the internet. LEAs incur substantial costs in detection and investigation of criminal activity. These law enforcement costs are ultimately borne by taxpayers. This Code endeavours to set clear procedures for cooperation between ISPs and LEAS in an effort to ensure that all these costs are minimised and equitably allocated. This Code is also an important part of internet industry initiatives to assist end users to address concerns that they may have as to risks of dealing online. These initiatives include education as to the availability and use of more secure methods of payment, virus protection software and personal firewalls.

1.7 This Code is, in the first instance, directed towards ISP/LEA cooperation. Nevertheless, the parties acknowledge the prospect of future extension to other areas of online activity, including hosting and e-commerce (reflecting the breadth of the IIA membership), provided always that such cooperation is solely directed to the purpose of addressing criminal or terrorist activity occurring on or by means of the internet and remains within the spirit and letter of relevant privacy legislation and IIA codes.

1.8 Either LEAs or ISPs can initiate interaction with each other in respect of an investigation. This Code seeks to set out procedures to ensure that all parties interact lawfully and in accordance with legitimate and reasonable expectations of those parties and of end users, thus affording parties a measure of certainty regarding the execution of LEA investigations.

1.9 The primary piece of legislation which governs ISPs in Australia is the *Telecommunications Act (C'th) 1997* (**the Act**). The Act covers a range of matters and obligations that ISPs should follow to assist LEAs in certain investigation activities. These matters are covered by Parts 13, 14 and 15 of the Act. The Act also operates

in conjunction with the *Telecommunications (Interception) Act (C'th) 1979* (**Interception Act**). This Code is not intended to deal with telecommunication interception obligations of CSPs, other than in referring to when a Telecommunications Interception (TI) Warrant is required, or not required.

1.10 Parts 13 and 14 of the Act respectively deal with Protection of Communications and National Interest Matters. The simplified outline of Part 13 reads as follows:

> *Carriers, carriage service providers, number-database operators, emergency call persons and their respective associates must protect the confidentiality of information that relates to:*
>
> *(a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and*
>
> *(b) carriage services supplied by carriers and carriage service providers; and*
>
> *(c) the affairs or personal particulars of other persons.*
>
> *The disclosure or use of protected information is authorised in limited circumstances (for example, disclosure or use for purposes relating to the enforcement of the criminal law).*
>
> *An authorised recipient of protected information may only disclose or use the information for an authorised purpose.*
>
> *Certain record-keeping requirements are imposed in relation to authorised disclosures or uses of information.*

1.11 The simplified outline of Part 14 reads as follows:

> *The ACA, carriers and carriage service providers must do their best to prevent telecommunications networks and facilities from being used to commit offences.*
>
> *The ACA, carriers and carriage service providers must give the authorities such help as is "***reasonably necessary***"[emphasis added] for the purposes of:*
>
> *(a) enforcing the criminal law and laws imposing pecuniary penalties; and*
>
> *(b) protecting the public revenue; and*

(c) safeguarding national security.

A carriage service provider may suspend the supply of a carriage service in an emergency if requested to do so by a senior police officer.

1.12 The simplified outline of Part 15 reads as follows:

Carriers and carriage service providers must comply with obligations concerning interception capability and special assistance capability.

Exemption from compliance with these obligations may be granted in certain circumstances.

Carriers and certain nominated carriage service providers must comply with the obligations to prepare and submit an annual interception capability plan.

Carriers and certain nominated carriage service providers must notify the ACA of technological changes affecting the provision of help under Part 14 in connection with a requirement under Division 2 of this Part.

Carriers and certain nominated carriage service providers must comply with obligations concerning agency specific delivery capability.

Carriers, carriage service providers and agencies are required to meet different costs associated with the provision of various capabilities related to interception.

The Minister is to conduct a review of the cost-effectiveness of interception.

1.13 An ISP is a carriage service provider for the purposes of the Act.

1.14 The Act is silent as to as to interpretation of the concept of "reasonably necessary" which is central to operation of both Parts 13 and 14 of the Act.

1.15 There has been confusion and uncertainty created by failing to have any clear guidelines available to the Internet industry and LEAs as to what constitutes "such help as is reasonably necessary" under the Act and how such assistance can be given and received so as to ensure that:

(a) LEAs receive legitimate assistance that they reasonably require;

(b) the administrative burdens placed on ISPs by these obligations are controlled; and

(c) ISPs and their staff are aware of their obligations and the parameters of the Act and thereby are not unreasonably exposed to criminal liability for failure to protect the privacy of communications of end users.

2. OTHER RELEVANT CODES AND INFORMATION SHEETS

2.1 This Code supplements other documents, such as Australian Communications Authority (**ACA**) Information Sheets and Law Enforcement Cooperation Manual, which are relevant to the obligations of ISPs in relation to the assistance which must be supplied to LEAs in accordance with the Act.

2.2 The booklet "Know Your Obligations" was prepared by the ACA as a guide to the key obligations placed on carriers and carriage service providers including ISPs, under the Act.

2.3 The ACA has also prepared a number of Industry Fact Sheets including "Internet service providers and law enforcement and national security", "ISP Interception Obligations" and "Carrier and Service Provider Regulation".

2.4 Further, the IIA has published a Fact Sheet for ISPs on Law Enforcement Cooperation at www.iia.net.au/ispsheet.html.

2.5 This Code does not seek to duplicate matters already dealt with by the booklet and fact sheets referred to in sections 2.2 to 2.3.

2.6 The documents referred to in sections 2.2 to 2.3 above are hereby incorporated into this Code by reference.

3. OBJECTIVES OF THIS CODE

3.1 The aims of this Code include to:

(a) establish a cooperative working environment for ISPs and LEAs in which there are clear policies and procedures relating to investigations into certain types of criminal and

civil acts having regard to the Act – in other words, to describe standards of best practice in relation to these matters;

(b) provide clear guidelines to the satisfaction of both industry and LEAs as to what constitutes "such help as is reasonably necessary" and to ensure this term is defined having regard to standards of confidentiality and privacy afforded to users of the Internet under the Act and thereby establish confidence in and encourage the use of the Internet;

(c) provide a transparent mechanism for the handling of LEA's investigations for the Internet industry and ensure that there is a clear understanding on both sides as to what the procedures are;

(d) promote positive relations between the LEAs and the Internet industry.

(e) give users of the Internet confidence that their privacy and the confidentiality of their transactions will be guarded from unlawful intrusion by LEAs.

4. PRINCIPLES UNDERLYING THIS CODE

4.1 In seeking to achieve its objectives this Code applies the following principles:

(a) the Code should be technology neutral;

(b) requirements should be fair to all concerned;

(c) requirements should not adversely affect the economic viability of the parties to the Code and the services they make available;

(d) all lawful privacy obligations will be respected.

5. TERMINOLOGY AND INTERPRETATION

5.1 In this Code:

ACA	means the Australian Communications Authority.

ACIF	means the Australian Communications Industry Forum.
Act	means the *Telecommunications Act, (C'th) 1997*.
Agency	means a department or other instrumentality of the Commonwealth of Australia, a State or Territory.
Authorised Officer	in relation to a LEA, means a Senior Officer of the Agency authorised in writing by the head of the Agency to issue certificates for the purposes of requesting the release of information under section 282 of the Act.
Carriage Service Provider	has the meaning given in section 7 of the Act and includes Internet Service Providers.
Certificate	means a certificate issued under subsections 282 (3), (4) or (5) of the Act.
Civil penalty-enforcement Agency	an agency responsible for administering a law imposing a pecuniary penalty.
CLI	Caller Line Identification is information that is generated by the network at the time a telephone call is established, and includes: • the called party's phone number • the calling party's phone number • the time of day • the duration of the call • the routing of the call.

CND	Caller Number Display is information contained in the signalling data which displays the originating caller's number on the terminating party's CND-enabled device (eg a home telephone equipped with a CND capacity). CND will not be displayed if the calling party has (temporarily or permanently) disabled CND or if the called party has not elected to pay for the CND service.
Criminal penalty-enforcement Agency	a) the Australian Federal Police; or b) a police force or service of a State or a Territory; or c) the National Crime Authority; or d) the New South Wales Crime Commission; or e) the Independent Commission Against Corruption of New South Wales; or f) the Crime and Misconduct Commission of Queensland; or g) a prescribed authority established by or under a law of Commonwealth, a State or Territory; or h) a body or organisation responsible to the Australasian Police Ministers' Council for the facilitation of national law enforcement support and includes the National Exchange of Police Information.
Code	means this Code of Practice.
Customer	means a person who subscribes for and to whom an ISP provides

	Internet access. Unless the context requires otherwise, a reference to a thing done by a Customer includes a thing done by a third party through that Customer's ISP account.
IIA	means the Internet Industry Association (ACN 071 075 575).
Interception Act	means the *Telecommunications (Interception) Act, (C'th) 1979*.
Internet	means the public network of computer networks known by that name which enables the transmission of information between users or between users and a place on the network.
Internet Service Provider	means a Carriage Service Provider who provides access to Internet services to the public.
LEAs	means collectively Civil Penalty Enforcement Agencies, Public Revenue Agencies, National Security Agencies, and Criminal Penalty Enforcement Agencies.
Other Authorised Process	means general search warrants and other notices and documents authorised by or under law or issued as a result of legal proceedings.
Personal Data	as defined in the *Privacy Amendment (Private Sector) Act (C'th) 2000* means the information, whether fact or opinion or evaluative material, about an identifiable individual that is recorded in any form.

POP	means Point of Presence and is the physical access location into a network.
Privacy Act	means the *Privacy Act (C'th) 1988* as amended by the *Privacy Amendment (Private Sector) Act (C'th) 2000*.
Public Revenue Agency	means an agency responsible for the administration of a law relating to the protection of the public revenue, and includes the Australian Taxation Office.
Senior Officer	in relation to a LEA, means: (a) if the agency is a police force or service – a commissioned officer of that force or service; (b) if the agency has a senior executive service (however described) – an officer of that service; (c) if the agency does not have a senior executive service (however described) – an officer of the agency (by whatever name called) who is concerned in, or takes part in, the management of the agency; (d) if a group of officers of the agency perform their duties at premises that are: (i) occupied by the agency; and (ii) located at a place outside the boundaries of a capital city of a State or internal Territory; the most senior of that group of officers.

	For the purposes of paragraph (d) the boundaries of a capital city are to be ascertained in accordance with the regulations. However, if no regulations are in force, the boundary of a capital city is a circle with a 50 kilometre radius from the general post office of the capital city.
Spoofing	forging an email header to make it appear as if it came from somewhere or someone other than the actual source
TI Warrant	for the purposes of this Code means a Telecommunications Interception warrant validly issued under the Interception Act

5.2 In this Code where examples are provided of the manner in which a Code provision may be satisfied, these examples should not be read as limiting the manner in which the provision may be satisfied.

6. PRIVACY ACT

6.1 ISPs who are not already subject to the Privacy Act may only subscribe to the Code if the IIA has been provided with written evidence that the ISP has elected to be treated as an organisation in accordance with section 6EA of the Privacy Act.

7. ISP RECORD KEEPING OBLIGATIONS IN RELATION TO PROVISION OF ASSISTANCE TO LEAS

Personal Data

7.1 The Act does not require ISPs to retain any particular records additional to those retained for the ordinary course of business. However there is a range of other legislative requirements that obliges Carriers and CSPs to retain financial records for approximate 7 years. Accordingly ISPs already have an obligation to provide reasonable assistance to LEAs under the

Act. In order to clarify this obligation ISPs will retain the following Customer related data (Personal Data):

(a) Customer name;

(b) username;

(c) email address;

(d) date of birth (if collected);

(e) Customer address;

(f) contact telephone numbers;

(g) type of service provided (dial, DSL etc);

(h) credit card details where credit card details are collected in relation to billing the particular service offered by the ISP;

(i) billing records;

(j) history of changes to Customer details;

(k) prepaid identifier (if applicable);

(l) sub-account details (if applicable).

7.2 Most ISP accounts are established following an application made by a prospective customer either by entering customer details online or through completion of a paper-based application form that is submitted to an ISP. Where these details, including any paper-based application form, are retained by an ISP, these details will also be Personal Data for the purposes of this Code.

7.3 ISPs may provide internet access services on a pre-paid basis or otherwise in circumstances where the person proposing to use these internet access services does not provide identity-related information at the point of sale or other provision of pre-paid access. Where internet access services are so provided, as soon as practicable after a prospective user logs on to an ISP's network the ISP will request the Customer to provide the Customer's name, residential address, contact telephone number, date of birth and the public number of any fixed line telephone service at the Customer's address. Where these details, including any paper-based application form, are retained by an ISP, these details will also be Personal Data for the purposes of this Code.

Operational Data

7.4 ISPs will retain the following operational data about each Customer and their interaction with the ISP's network (Operational Data):

(a) dynamic IP allocation records, indicating which IP address was assigned to which Customer account at specific log in times;

(b) records of the date and time of each log in and log out of a Customer;

(c) CND or CLI where collected;

(d) total data transferred (if collected)

Other Data

7.5 ISPs will retain the following other data (if collected) about each Customer and their interaction with the ISP's network (Other Data):

(a) proxy logs (IP Address, Time, URL);

(b) email Arrival, delivery, sender, recipient, size;

(c) newsgroup logs;

(d) FTP logs.

7.6 LEAs understand that ISPs cannot verify the identity of a person using a Customer's log-in details. LEAs also understand that CLI information is generally not made available to ISPs at this stage. Accordingly, ISPs cannot verify whether:

(a) Personal Data provided by a Customer is accurate in every respect;

(b) a Customer has logged in using any particular and identifiable phone service or line.

7.7 The information referred to in sections 7.1, 7.4 and 7.5 will be retained by the ISP for the purposes of this Code for a minimum period of:

(a) for Personal Data, 6 months from the date a Customer ceases to be Customer, or for 12 months after the creation of the record; whichever is the greater;

(b) for Operational Data, 6 months from the date of creation of such data;

(c) for Other Data, 1 week after creation of the record.

This information will be retained by the ISP at the cost of the ISP and in a form determined by the ISP, such as electronic media or off-line storage such as CD-ROM, capable of being accessed and read by the ISP during the retention period.

7.8 The retention periods set out in section 7.7 are a minimum standard only and ISPs may retain Personal, Operational and Other Data for longer periods at their discretion whilst at all times complying with the Privacy Act.

7.9 ISPs will not be required, unless in response to a proper TI Warrant or Other Authorised Process, to retain or deliver to the LEAs information relating to the content or substance of any communications of its Customers (see further section 10 below).

7.10 ISPs will not be required, unless in response to a proper TI Warrant, Certificate or Other Authorised Process, to retain or deliver to the LEAs information relating to usage by a Customer of the ISP's services, including information as destination sites and particular tasks undertaken by a Customer during any session they are logged into the ISP's network.

8. ISP OBLIGATIONS IN RELATION TO PROVISION OF ASSISTANCE TO LEAS – LEA INITIATION OF REQUEST

8.1 LEAs will ordinarily initiate a request for disclosure of information or documents where a third party, such as a customer of an ISP, is a victim, suspect or witness of the particular matter being investigated. For example, where a person is suspected of committing a fraud or other criminal offence by 'spoofing' an email account maintained with an ISP, and a LEA requires details as to usage of that email account or the person in whose name

the email account is registered, the ISP may respond to a request made by the LEA for disclosure of information or documents.

8.2 Except as noted in section 8.3 below, LEAs should initiate all requests for information relating to carriage services supplied, or the affairs or personal particulars of a Customer, through the submission to the ISP of a Certificate issued pursuant to section 282 of the Act. Attached and marked "A" is a form of certificate which ISPs and LEAs agree is appropriate to satisfy the requirements of the ACA as well as achieve the purposes of the Act.

8.3 Information which may be requested pursuant to a Certificate includes Personal Data, Operational Data and Other Data as referred to in section 7 above.

8.4 The LEAs will submit the Certificate in accordance with the processes agreed in section 11 of this Code.

9. LEA OBLIGATIONS IN RELATION TO PROVISION OF ASSISTANCE TO ISPs - ISP INITIATION

9.1 While information would normally be provided to LEAs as a result of a request for assistance, the Act enables ISPs to disclose any information of their own volition which is reasonably necessary for one or more of the stated purposes in the Act. However, unless otherwise required by law, it is at the ISPs' sole discretion as to whether any such information is disclosed or any particular request is responded to.

9.2 ISPs would usually initiate a request for investigation where they believe themselves to be the victim. For example, where there is an allegation by a customer that a credit card account has been fraudulently used, and pursuant to a request made by that customer to a bank or other credit card issuer a charge incurred against that credit card has been "charged-back" to the ISP, the ISP may disclose to a relevant LEA information or documents about the circumstances in which the charge was incurred and as to any investigations that the ISP had undertaken to ascertain or verify the identity of the person incurring the charge LEAs require the reporting of any crime to be supported by relevant information and evidence, in accordance with section 11.2.

9.3 Interaction with LEAs shall take place in accordance with the processes set out in section 11.

10. CONTENT OF COMMUNICATIONS

10.1 Section 280 of the Act provides for Authorisation By or Under Law. Division 2 does not prohibit (ie make it an offence) the disclosure/use of information (including content) in connection with a law enforcement agency if it is required or authorised under TI Warrant or Other Authorised Process. This section does not expressly authorise the disclosure, it simply exempts the disclosure from the prohibition so that the disclosure under TI Warrant or Other Authorised Process will not amount to an offence under the Act. LEAs and ISPs agree that requests should not be made via a Certificate for the disclosure by a person of information or a document that relates to:

(a) the contents or substance of a communication that has been carried by an ISP; or

(b) the contents or substance of a communication that is being carried by a ISP (including a communication that has been collected or received by such an ISP for carriage by it but has not been delivered by it).

10.2 The Interception Act governs the access to communications which are in passage over the telecommunications system. If a communication is in passage over the telecommunications system, a LEA will require a TI Warrant. Where an ISP can satisfy itself that a communication has completed its passage over the telecommunications system, then a LEA may be granted access to the communications by some other lawful means such as Other Authorised Process.

10.3 Without limiting the concepts of 'content' or 'substance of communication', ISPs and LEAs agree that the following do constitute content and/or substance of communication:

(a) any voice message held as stored voicemail;

(b) the text message held as stored email;

(c) a posting to a newsgroup.

The "to" and "from" address line of an email, and any 'extended header' addressing information associated with routing a message from its originating point to its destination, is not content and/or substance of information. This information where

available may be provided by an ISP to a LEA pursuant to sections 7, 8 and 9 above.

11. PROCESSES FOR DISCLOSURE AND COOPERATION

11.1 ISPs will ensure that the following processes are in place for receiving and responding to all requests from LEAs under sections 282 and 283 of the Act for Customer information. These processes should ensure that:

(a) A person is nominated as primary point of contact in the ISP for interaction with LEAs. That person's business hours and out-of-hours contact details will be provided to the LEAs;

(b) An alternative or secondary point of contact is also nominated as a point of contact if the primary contact is unavailable for any reason. That person's business hours and out-of-hours contact details will be provided to the LEAs;

(c) Staff designated by the ISP to respond to a LEA request have been made available at the request of a LEA for police checks and security clearances as requested by the LEA;

(d) Requests by LEAs for assistance are dealt with promptly;

(e) Information disclosed in response to requests is forwarded in an agreed manner to a pre-arranged destination;

(f) Staff designated by the ISP to respond to a LEA request are fully briefed in relation to their obligations under Parts 13 and 14 of the Act and this Code.

11.2 ISPs will undertake the following procedures prior to contacting, or advising its Customers to contact a LEA in respect of any particular suspected criminal activity, including fraudulent activity or threat to national security:

(a) Run a detailed usage report on the both the complainant and the user alleged to be involved in the suspected activity. It is recognised that the complainant and the user will in most case be the same;

(b) Analyse the report created pursuant to (a) to check for suspicious activity such as concurrent log ons or unusual variances in usage patterns;

(c) Attempt to verify legitimate usage of the account by checking for CLI;

(d) Liaise directly with the complainant to gain an understanding of their usage of the account including:

- home/office use
- who has access to the account
- whether there are any children/staff with access (or possible access) to the account
- whether the access is by a laptop or PC
- CND of lines used to access the account
- password procedures – storage/knowledge
- use of chat services and the like;

(e) Review of POP/server information available with respect to the account to locate evidence of any unusual use – for example access to a NSW account from a Victorian POP.

11.3 LEAs will ensure that the following processes are in place for receiving and responding to all requests from ISPs for investigations. These processes should ensure that:

(a) A central point of contact in the LEA for dealing with any issue or concern as to any interaction between a LEA and a particular ISP. Relevant business hours and out-of-hours contact details will be provided to the ISP;

(b) An alternative or secondary point of contact will also be nominated as a point of contact if the primary contact is unavailable for any reason. That person's business hours and out-of-hours contact details will be provided to the ISP;

(c) Requests by ISPs for assistance in investigation of fraud or other illegal activity are dealt with quickly and efficiently, provided that the ISP provides all reasonable assistance to enable this investigation to be undertaken, including, where possible, the assistance identified in section 11.2;

(d) Information required in response to investigation requests is despatched in an agreed manner to a pre-arranged destination.

12. RECOVERY OF COSTS

12.1 Section 314 of the Act outlines terms and conditions upon which assistance is to be given by carriage service providers such as ISPs to LEAs. Essentially, assistance is generally to be given on the basis that ISPs do not profit from, nor bear the cost of giving, that assistance.

12.2 Section 314 also makes provision for LEAs and ISPs to negotiate the costs of providing the assistance, based on principles of cost allocation governed by the nature and extent of requirements in each case. If an agreement cannot be reached, the appropriate costs are to be determined by an Arbitrator (appointed by the parties, or by the ACA in the absence of agreement). ISPs must not include in their cost recovery calculations from LEAs any cost incurred in compliance with regulations and determinations. ISPs may only seek payment for those costs directly incurred as a result of the provision of assistance to LEAs.

12.3 In determining whether a charge for assistance is reasonable the parties should take into account the following guidelines:

(a) whether the assistance must be provided outside normal working hours;

(b) whether the request is framed to take account of the way information is retained by an ISP or otherwise complies with requirements of this Code;

(c) whether the information requested is readily available on-line within an ISP's systems or whether this information must be retrieved from off-line storage or otherwise requires archival searching;

(d) how long the request took;

(e) the level and extent of staff involvement; and

(f) any additional costs for the provision of urgent or higher priority assistance.

13. SECURITY AND EVIDENCE HANDLING PROCEDURES

13.1 In order to assist LEAs by providing them with useful evidence the Internet Engineering Task Force Guidelines Evidence Collection and Handling should, to the extent possible and relevant, be followed by ISPs as part of their security practices and procedures. A copy of the Guidelines is attached to this Code and marked "B"

14. INTELLIGENCE SHARING

14.1 ISPs under this Code are encouraged to report instances of criminal activity online through an incident reporting scheme through such forums as the IIA establishes or, where one arises separately, makes known.

Attachments

"A"- form of certificate which ISPs and LEAs agree is appropriate to satisfy the requirements of the ACA as well as achieve the purposes of the Act (section 7.2) To be attached

"B" – Evidence Collection and Handling Guidelines

“B”

November 2001 - Internet Engineering Task Force

Guidelines for Evidence Collection and Archiving

Abstract

A "security incident" as defined in [RFC2828] is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident. If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

1. Introduction

A "security incident" as defined in [RFC2828] is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident. It's not our intention to insist that all System Administrators rigidly follow these guidelines every time they have a security incident. Rather, we want to provide guidance on what they should do if they elect to collect and protect information relating to an intrusion.

Such collection represents a considerable effort on the part of the System Administrator. Great progress has been made in recent years to speed up the re-installation of the Operating System and to facilitate the reversion of a system to a 'known' state, thus making the 'easy option' even more attractive. Meanwhile little has been done to provide easy ways of archiving evidence (the difficult option). Further, increasing disk and memory capacities and the more widespread use of stealth and cover-your-tracks tactics by attackers have exacerbated the problem.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

You should use these guidelines as a basis for formulating your site's evidence collection procedures, and should incorporate your site's procedures into your Incident Handling documentation. The guidelines in this document may not be appropriate under all

jurisdictions. Once you've formulated your site's evidence collection procedures, you should have law enforcement for your jurisdiction confirm that they're adequate.

1.1 Conventions Used in this Document

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

2. Guiding Principles during Evidence Collection.

- Adhere to your site's Security Policy and engage the appropriate Incident Handling and Law Enforcement personnel.
- Capture as accurate a picture of the system as possible. - Keep detailed notes. These should include dates and times. If possible generate an automatic transcript. (e.g., On Unix systems the 'script' program can be used, however the output file it generates should not be to media that is part of the evidence). Notes and print-outs should be signed and dated.
- Note the difference between the system clock and UTC. For each timestamp provided, indicate whether UTC or local time is used. - Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.
- Minimise changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times. - Remove external avenues for change. - When confronted with a choice between collection and analysis you should do collection first and analysis later. - Though it hardly needs stating, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly in a crisis. If possible procedures should be automated for reasons of speed and accuracy. Be methodical.
- For each device, a methodical approach should be adopted which follows the guidelines laid down in your collection procedure. Speed will often be critical so where there are a number of devices requiring examination it may be appropriate to spread the work among your team to collect the evidence in parallel. However on a single given system collection should be done step by step.

- Proceed from the volatile to the less volatile (see the Order of Volatility below).
- You should make a bit-level copy of the system's media. If you wish to do forensics analysis you should make a bit-level copy of your evidence copy for that purpose, as your analysis will almost certainly alter file access times. Avoid doing forensics on the evidence copy.

2.1 Order of Volatility

When collecting evidence you should proceed from the volatile to the less volatile. Here is an example order of volatility for a typical system.

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

2.2 Things to avoid

It's all too easy to destroy evidence, however inadvertently.

- Don't shutdown until you've completed evidence collection. Much evidence may be lost and the attacker may have altered the startup/shutdown scripts/services to destroy evidence.
- Don't trust the programs on the system. Run your evidence gathering programs from appropriately protected media (see below).
- Don't run programs that modify the access time of all files on the system (e.g., 'tar' or 'xcopy'). - When removing external avenues for change note that simply disconnecting or filtering from the network may trigger "deadman switches" that detect when they're off the net and wipe evidence.

2.3 Privacy Considerations

- Respect the privacy rules and guidelines of your company and your legal jurisdiction. In particular, make sure no information collected along with the evidence

you are searching for is available to anyone who would not normally have access to this information. This includes access to log files (which may reveal patterns of user behaviour) as well as personal data files.

- Do not intrude on people's privacy without strong justification. In particular, do not collect information from areas you do not normally have reason to access (such as personal file stores) unless you have sufficient indication that there is a real incident.
- Make sure you have the backing of your company's established procedures in taking the steps you do to collect evidence of an incident.

2.4 Legal Considerations

Computer evidence needs to be

- Admissible: It must conform to certain legal rules before it can be put before a court.
- Authentic: It must be possible to positively tie evidentiary material to the incident.
- Complete: It must tell the whole story and not just a particular perspective.
- Reliable: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- Believable: It must be readily believable and understandable by a court.

3. The Collection Procedure

Your collection procedures should be as detailed as possible. As is the case with your overall Incident Handling procedures, they should be unambiguous, and should minimise the amount of decision-making needed during the collection process.

3.1 Transparency

The methods used to collect evidence should be transparent and reproducible. You should be prepared to reproduce precisely the methods you used, and have those methods tested by independent experts.

3.2 Collection Steps

- Where is the evidence? List what systems were involved in the incident and from which evidence will be collected.
- Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.
- For each system, obtain the relevant order of volatility.
- Remove external avenues for change.
- Following the order of volatility, collect the evidence with tools as discussed in Section 5.
- Record the extent of the system's clock drift.
- Question what else may be evidence as you work through the collection steps. - Document each step.
- Don't forget the people involved. Make notes of who was there and what were they doing, what they observed and how they reacted.

Where feasible you should consider generating checksums and cryptographically signing the collected evidence, as this may make it easier to preserve a strong chain of evidence. In doing so you must not alter the evidence.

4. The Archiving Procedure

Evidence must be strictly secured. In addition, the Chain of Custody needs to be clearly documented.

4.1 Chain of Custody

You should be able to clearly describe how the evidence was found, how it was handled and everything that happened to it. The following need to be documented:

- Where, when and by whom was the evidence discovered and collected.
- Where, when and by whom was the evidence handled or examined.
- Who had custody of the evidence, during what period. How was it stored.
- When the evidence changed custody, when and how did the transfer occur (include shipping numbers, etc.).

4.2 Where and how to Archive

If possible commonly used media (rather than some obscure storage media) should be used for archiving. Access to

evidence should be extremely restricted, and should be clearly documented. It should be possible to detect unauthorised access.

5. Tools you'll need

You should have the programs you need to do evidence collection and forensics on read-only media (e.g., a CD). You should have prepared such a set of tools for each of the Operating Systems that you manage in advance of having to use it. Your set of tools should include the following:

- a program for examining processes (e.g., 'ps').
- programs for examining system state (e.g., 'showrev', 'ifconfig', 'netstat', 'arp').
- a program for doing bit-to-bit copies (e.g., 'dd', 'SafeBack').
- programs for generating checksums and signatures (e.g., 'sha1sum', a checksum-enabled 'dd', 'SafeBack', 'pgp').
- programs for generating core images and for examining them (e.g., 'gcore', 'gdb').
- scripts to automate evidence collection (e.g., The Coroner's Toolkit [FAR1999]).

The programs in your set of tools should be statically linked, and should not require the use of any libraries other than those on the read-only media. Even then, since modern rootkits may be installed through loadable kernel modules, you should consider that your tools might not be giving you a full picture of the system.

You should be prepared to testify to the authenticity and reliability of the tools that you use.

6. References

[FAR1999]
Farmer, D., and W Venema, "Computer Forensics Analysis Class Handouts", http://www.fish.com/forensics/

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2196] Fraser, B., "Site Security Handbook", RFC 2196, September 1997.

[RFC2350] Brownlee, N., and E. Guttman, "Expectations for Computer Security Incident Response", RFC 2350, June 1998.

[RFC2828] Shirey, R., "Internet Security Glossary", RFC 2828, May 2000.

7 Acknowledgements

We gratefully acknowledge the constructive comments received from Harald Alvestrand, Byron Collie, Barbara Y. Fraser, Gordon Lennox, Andrew Rees, Steve Romig and Floyd Short.

8 Security Considerations

This entire document discusses security issues.

9 Full Copyright Statement