Paul Wright:

Should corporate management include a Computer Forensics and Incident Response capability into realigned Information Security Principles?

Abstract:

IT enabled abuse and data compromise is a major problem to senior management and organisations as a whole. It has no boundaries, and globally undermines electronic commerce whilst being facilitated by the rapid development of the Internet, computer and information technology. The prevention, reporting, detection and our ability to investigate is of overriding importance to a range of institutions and establishments. Currently the full extent of the problem is not known and at present cannot be scoped; however there is substantial evidence that shows it to be on the increase. Despite historical reports such as the Council of Europe report on Cyber crime (2001)[17] that indicated there would be an increase in criminal offences that exploit the opportunities presented by the globalisation of computer networks.

Agenda

Author(s):

Paul Wright, MSc, EnCE, CFIA, CSTA:

- Organization and contact address: e-crime consultancy, PO Box 4400, Toddington, Dunstable, England LU5 6WE
- Telephone, email and personal homepage: ☎ +44 7973 672918, ✉ paulwright@e-crimeconsultancy.co.uk, 💻 www.e-crimeconsultancy.co.uk

[17] Council of Europe (2001) CETS No.185 Convention on Cybercrime. Budapest. 23/11/2001Petherick, W. (2001). Criminal Profiling. USA. Crime Library

ISSN 1614-1687

Introduction

Firstly, it will be argued that senior management should realign the primary objectives of information security from a focus on the principles of confidentiality, integrity, and availability (CIA) to risk and exposure assessments, and vulnerability testing. Secondly, and more importantly, the incorporation of a computer forensic capability, an incident response procedure and the use of digital intelligence within any information security strategy will be advocated. Then, having produced the evidence to support this, a number of recommendations on how to implement such strategies will be proposed.

Information is a valuable asset to any organisation, and those that use it for e-commerce are now being affected by the challenges of IT enabled abuse, in particular data compromise. In some instances the technological developments and innovative mind of the abuser are leaving information security and legal systems playing catch up.

This results in the persistent occurrence of IT abuse and data compromise globally, causing serious financial loss and reputational damage to organisations and the individual. The source of this data comes from large-scale compromise incidents at a corporate level, yet still the spotlight tends to focus upon the individual.[18]

The other drawback when scoping IT abuse and data compromise is the fact that the availability of information is limited and all too regularly it is defined anecdotally from a small number of well-known incidents. At other times, questionable, optimistic or negative estimates are presented as fact. Some organisations believe that a thorough and methodical approach to the collation and analysis of compromise incident information will give up a more accurate evaluation of the circumstances and in time will produce a more reliable understanding of this problem.

To protect themselves, organisations need to be encouraged to invest in an Information Security Management System (ISMS). By implementing said systems organisations will at the same time go towards compliance with Principles 2 and 3 of the Financial Services Authority's (FSA) report in 2007 entitled "*Principles-Based Regulation*".[19] Noting that the FSA clarifies this by stating that all organisations' handling of data in both the public and private sectors can benefit from its advice.

Principle 2 requires "that a firm must conduct its business with due skill, care and diligence."

Principle 3 that "a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

Currently, the main objectives of information management are confidentiality, integrity and availability, not forgetting accountability and accessibility. Do these objectives enable organisations to protect themselves while being able to respond to incidents and disseminate digital intelligence so others can act upon it?

The FSA in their recent report on "*Data Security and the Financial Services*" [20] have consolidated examples of poor practice in data security, for example:

1. No training to communicate policies and procedures.
2. Temporary staff receiving less-rigorous vetting than permanently employed colleagues carrying out similar roles.
3. Failing to consider continually whether employees in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.
4. Failing to monitor super users or other employees with access to large amounts of customer data.
5. Firms stockpiling obsolete computers and other portable media for too long and in insecure environments.

Surely a robust e-crime prevention approach and the establishment of e-crime prevention positions could target these areas and more?

[18] http://news.bbc.co.uk/1/hi/uk_politics/7667507.stm

[19] http://www.fsa.gov.uk/pubs/other/principles.pdf

[20] Data Security in Financial Services 2008 [Online] http://www.fsa.gov.uk/pubs/other/data_security.pdf

What do we know?

Historical evidence on how organised offenders work can be found on the Internet, one incident in particular was when a person using the nickname *'Reverse'* was interviewed and he/she stated;

> *"We have a group of professional hackers/fraudsters/legal bankers, we share information, but if we work together also revenues".*
>
> *"My name is 'Script', I'm a founder of forum.carderplanet.net and I can provide you with excellent credit cards with cvv2 code and without it, minimum deal is a USD $200.00" (Script, 2003)*[21].

A report from the Information Assurance Advisory Council (IAAC) claims that companies are not able to collect digital evidence properly, and as a consequence any prosecution is not straightforward. The IAAC have responded by releasing guidelines to assist companies in capturing and preserving electronic evidence in a way that makes it admissible in court. "Effective detection and prosecution have a central role to play in deterrence", said Pauline Neville Jones, Chair of the IAAC (Sommer, 2005)[22].

An important point is that organisations and individuals must recognise that whatever analysis they carry out and whatever policies and procedures are implemented, they will quickly become out of date. Moreover, this also includes how the investigator carries out digital analysis of computer media.

In the meantime, very few managers are happy to admit that they have had serious information security issues in their organisations and as a consequence that they must expect there will be more breaches in the future, and they will be harder to detect. As with legislation, the adoption of security controls is not keeping pace with the growing use of new technologies. Organisations are becoming dependent upon a complex web of worldwide information infrastructures, without necessarily understanding or quantifying the risks or their exposure to the same.

It is readily acknowledged that some organisations have tried and tested policies, procedures and best practices to combat data compromise. Unfortunately investigative experience shows us that this is not always the case and that there are internal organisational voids and single points of failure that facilitate such compromise.

When an incident occurs there is a strong tendency to have staff 'take a quick look' at the computers involved in an attempt to confirm or deny suspicions. Unfortunately, this act, if not carried out using proper protocols will result in changes to data that damage forensic evidence[23]. IT professionals are well informed about their organisations' systems, data locations, media types, software use and data retention policies. Nonetheless, this wealth of information does not give rise to an expertise in the area of e-data compromise or computer forensics.

Illegal on-line techniques and illegal electronic searching of an organisation's data are being used to obtain sensitive documents. The wealth of the supply can be substantiated by looking at the chronology of data breaches available on the privacyrights.org website[24] It indicates the extent of the problem, for example, from January 2005 till January 2009, the said website records a total of over 252,000,000 identities as having been lost. These incidents are mainly located in the United States; on the other hand, if breaches from the rest of the world were included the total number would be appreciably higher.

Recent high profile financial investigations involving global organisations demonstrate the pivotal role that electronic data can play in legal disputes and investigations. Organisations that choose to ignore this vital evidence risk severe reputational damage and financial penalties. These events and the recent

[21] Script. (2003, January 22) you can buy credit cards on www.carderplanet.net. Message posted FORUM.CARDERPLANET.NET. Retrieved October 18 2006 from http://lists.debian.org/debian-hurd/2003/01/msg00075.html

[22] Sommer, Peter. (2005) Directors and Corporate Advisors Guide to Digital Investigations and Evidence. Information Assurance Advisory Council www.iaac.org.uk

[23] ACPO (Version 4.0) Good Practice Guide for Computer based Electronic Evidence, Association of Police Chief Officers. [Online] http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

[24] http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

loss of data from the Child Benefit Agency[25] and the Nationwide Building Society[26] have raised the growing profile of identity theft and what it can cost a company. The FSA fined the Nationwide £980,000.

The focus to date has been on how individuals can protect themselves by shredding documentation and showing extra caution when divulging personal details. However, while rising levels of consumer awareness should be welcomed and encouraged, the focus on the individual is not the way forward. One of the major sources of customer information for the offender comes from large-scale data compromise and identity theft incidents at a corporate level.[27] Confidential data such as consumer details, intellectual property and financially sensitive information all have a fundamental value.[28]

It is important to note that when missing data is retrieved, if the data was not protected i.e. encrypted, there is no assurance that it has not already been duplicated, stored elsewhere, or forwarded to another for illicit purposes. In addition, in 2007 data loss was reported to be the most common type of financial crime reported to the FSA, who also judged it to be highly likely that many data losses are not identified or go unreported.[29]

Trends

Firstly, a large number of organisations are failing to recognise all aspects of the security risks that they are exposed to. Some just do not realise the magnitude of the risk, while others do not have the know-how to mitigate their vulnerability and countless fail to provide sufficient resources to lessen the risk.

Secondly, the enormous volume of data concerned in a typical compromise incident practically assures that those involved have a plentiful supply of information and intelligence, which is the foundation for many illegal endeavours. This endless supply of high quality data virtually guarantees that for the foreseeable future IT abuse and data compromises will remain a profitable business. It is also useful to recognise that immoral individuals will respond to opportunities rapidly and tend to exploit emerging opportunities much faster than most organisations can design and implement security controls.

Then there is a 'reputational damage' bias in any statistics. This is due to the fact that a significant number of organisations consistently fail to report information and therefore cause an under representation in the available figures. Additionally, those developing organisations that lack any Information Security Management System (ISMS) have an inadequate ability to detect and report data compromises.

More recently, we have seen another trend where security cleared staff contravened internal policies and procedures by looking at information relating to celebrities, committed fraud or were coerced into giving data to criminals or allowing them access to the same.[30]

Investigative Ability

IT abuse and data compromise is committed across cyberspace and does not stop at national borders. More than with any other global crime, the swiftness and flexibility of IT abuse and data compromise challenge the existing rules of regulation and legislation. It can be perpetrated from anywhere in the world against any computer, and it is recognised that efficient action to combat it is necessary at not only a local level but also at a global level.

Legislation has fallen behind; it needs to maintain the same speed of change as *"Moore's Law"*[31]. The international legal systems have gone some way to achieve this with the sixth principle[32] established by G8, commonly known as *"Quick freeze, slow*

---

25 http://news.bbc.co.uk/2/hi/uk_news/politics/7104840.stm

26 http://news.bbc.co.uk/1/hi/business/6360715.stm

27 http://news.bbc.co.uk/1/hi/uk/7449927.stm

28 http://money.aol.co.uk/credit-report-centre/bank-details-sold-on-internet/article/20071203012409990001

29 Page 15, Data Security in Financial Services 2008 [Online] http://www.fsa.gov.uk/pubs/other/data_security.pdf

30 http://www.guardian.co.uk/world/2008/mar/21/barackobama.uselections2008

31 http://en.wikipedia.org/wiki/Moore%27s_law

32 Meeting of the Justice and Interior Ministers of the Eight December 9th -10th, 1997

thaw'[33]. Despite this the detection and punishment of cybercrime is highly likely to remain problematic.

Then consider that alongside the fact that, despite a clear need for consistent legislation around the world to facilitate international investigations, there are major differences between the legal systems and cultures, making legislative consistency difficult. The implementation of *'Corpus Juris'* is a long way off.[34]

Organisations are becoming dependent upon a complex web of global information infrastructures, without necessarily understanding or quantifying the risks. The damaging results of an incident can be minimised if an organisation is pro-active and innovative in putting itself in a position to lessen the cost of any investigation, and penalties that are related to the exposure of valuable data. The scope of the problem may be larger than first perceived and untrained staff may overlook significant lines of investigation, which then leaves the organisation vulnerable to a reoccurrence of the same incident. Therefore, policies need to be established with regard to company computers and networks to provide a line of authority for the conducting of such an investigation.

As always, the quandary of target-based investigations is that funding decisions are based on tick box results, good clear-up figures and value for money. By contrast, there's little or no motivation to invest in e-crime investigations and forensics when the offences are extremely complex to investigate and the probability of a successful conclusion are restricted, especially as offenders and evidence are often located overseas.

Peter Sommer has responded to Minister Hazel Blears recent announcement of £70 million spent on funding websites to target Muslims in a bid to counter the threat of web-based extremism[35] by stating, *"How can that sort of money be justified when there are areas of e-crime crying out for cash, but not getting a penny? It's outrageous,"*

Previous investigations and business presentations can confirm that organisations could do more and are definitely vulnerable to e-crime and IT abuse. Would an e-crime advice centre linked to the chamber of commerce be a way forward? Has the National e-Crime Prevention Centre (NeCPC) got it right?[36] Will we be playing 'catch-up' when the Police Central e-Crime Unit (PCeU) is established in 2009?[37]

Lack of Intelligence Analysis

Many make out that there are limitations to the information and intelligence that can be gathered; there is not, there is only a need to balance, risk assess and evaluate one's ability to gather digital intelligence – know thy enemy.

In these circumstances, knowing your foe is no longer an option – it's a necessity. If organisations do not know their enemy and are unaware of current trends and techniques, it becomes difficult to see how effective controls, procedures and policies can realistically be put in place. For example, how many organisations routinely harvest the criminal intelligence that is openly available to anyone with access to the Internet? How many organisations know how to monitor criminal data markets so that they can see if any of their corporate data is being offered for sale, thus indicating that they have had a security breach? In addition, without an understanding of the way the high-tech abuser thinks, it becomes difficult to anticipate future attacks.

This is where senior management has to have an understanding of the offender's modus operandi for

[33] "Quick freeze, slow thaw" arrangement by which law enforcement and judicial bodies can fulfil their procedural obligations under domestic law for release of information to foreign law enforcement or judicial officials without risking the loss of critical data. http://media.hoover.org/documents/0817999825_35.pdf

[34] Wikipedia. Corpus Juris. The legal term Corpus Juris means "body of law". It was originally used by the Romans for several of their collections of all the laws in a certain field. Retrieved October 18 2006 from http://en.wikipedia.org/wiki/Corpus_juris

[35] "Political Pain". PC Pro 8th February 2008 http://www.pcpro.co.uk/features/164145/the-ecrime-epidemic/page3.html

[36] http://necpc.org.uk/

[37] http://www.computerweekly.com/Articles/2008/09/30/232508/government-pledges-funding-for-e-crime-unit.htm

acquiring data. This in turn will lead to a logical conclusion that international coordination and collaboration are not the only ways to address data compromise.

There is hard intelligence that data markets exist and are expanding and it is compounded when you combine this with the fact that the sheer volume of data involved in a typical compromise guarantees that the criminal has an abundant supply of individual and corporate information.

In addition some organisations have implemented a retrospective move towards information and data security risk assessments, and exposure assessments. They need a breach of security or data loss to have taken place before considering such risks, exposure and procedures to deal with the same. Without these, organisations will allocate their assets improperly and expose themselves, their clients and customers to preventable risk.

It is also worth noting that currently the works of those who produce investigative guidelines for e-crime tend to focus on detection and prosecution. They cover the specialist forensic and investigative work that is required to tackle IT abuse and e-crime, but give little attention to the area of e-crime prevention and intelligence analysis.

Incident Response

According to the ISO standard, *"information security is achieved by implementing a suitable set of controls"*[38]. It goes on to recommend that an organisation should establish procedures *"to ensure a quick, effective and orderly response to security incidents"*. These procedures should guarantee the reporting of an incident to an appropriate authority. The organisation that has suffered a security incident must properly collect evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings.

This requires that the evidence be collected in a forensically sound manner. The standard recognises this explicitly, as it notes that an organisation *"should ensure that their information systems comply with the requirements applicable to the production of admissible evidence. Indeed, to achieve quality and completeness of the evidence, a strong evidence trail is needed"*.[39]

If an organisation does not have the tools necessary to collect evidence in a manner that preserves its admissibility it risks compromising its legal, and as a consequence its financial situation.

When an incident is detected initially, it may not be apparent that it will result in civil or criminal court proceedings. Therefore, the danger exists that necessary evidence is destroyed accidentally before the seriousness of the incident is realised. Best practice utilises the standard to improve current information security controls and measures. An organisation must decide which strategy is most appropriate to match its business needs.

The integration of network and computer forensics into an information security programme can limit the exposure of critical and sensitive data in the event of a security breach. It can also facilitate an appropriate reaction and warning procedure so as to reduce exposure and liability.

A lack of understanding about computer forensics means that organisations are highly likely to handle any potential evidence in an improper manner. Such evidence needs to have been acquired in a forensically sound manner; failure to comply with the appropriate evidential handling procedure, civil or criminal, can result in no formal action being taken against a perpetrator. Note that criminal proceedings require a higher degree of proof.

The importance of forensic awareness and the employment of computer forensics when responding to an incident cannot be emphasised enough. Those that do prepare will put themselves ahead of the game when it comes to reducing costs and liabilities associated with the exposure of data.

Therefore extra investment in security, incident response and computer forensics is worthwhile, especially as many are now remarking on how the increased use of computers to commit offences produces a significant volume of electronic evidence for both civil and criminal proceedings. This in turn is causing problems to investigators due to the numerous places in which evidence can be located,

[38] http://www.27001-online.com/

[39] ditto

and the ease with which such evidence can become contaminated.[40]

> *"If there is even the slightest chance that your may prosecute an individual or organisation based on evidence obtained during your forensic investigation, I highly recommend that your obtain assistance from qualified forensic analysts and/or technology minded law enforcement officers."*[41]

Measuring the Effectiveness of Controls

So we need to be able to define how to measure the effectiveness of the selected controls, and to specify how these measurements are to be used to evaluate control efficiency to produce comparable and reproducible results. In other words, measuring the effectiveness of controls to verify that security requirements have, and can be been met.

One such tactic that can be successfully deployed is to conduct a focused exposure assessment to help identify areas where organisations are most exposed to the threat of data compromise. Exposure assessments are designed to get under the skin of potential control weaknesses and to examine existing control regimes with a view to identifying opportunities for unlawful activity. However, if there is not a genuine understanding of the way that criminals operate in this arena, then many potential control weaknesses may go undisclosed.

One way to benchmark data security is to use an International worth standard such as ISO 27001, a security management standard that was introduced in 2005 by the FSA.

Conclusion

Today, there are more organisations experiencing IT abuse and data compromise than ever before, and there are a wider variety of information security systems being breached. To go some way to fighting this, a significant number of organisations need to take steps to develop their incident response[42] procedures by improving their policies and forensic capabilities.

A business operating in multiple countries has to comply with a number of different and sometimes-contradictory legal constraints. This is a burden to an organisation and unfortunately it is highly unlikely to change in the anticipated future. Therefore if others are not going to provide legislative protection, we need to be groundbreaking and implement innovative organisational policies and procedures. We believe that realigned information security principles are one way of achieving this cross border, cross-jurisdictional problem, combined with the implementation of incident response.

This issue is a very important one from an organisational perspective because not only are there many legislative drivers regarding information security, there is evidence to show that share price is affected after a security breach and\or a data compromise incident being declared.[43]

One of the key reasons given by respondents to security surveys for not reporting data compromise and other hi-tech security breaches was the concern for reputational damage.[44] Therefore why not attack this cross road of ideals from another angle; join together in establishing a coordinated approach to the hi-tech and e-crime aspect of prevention and have all promote the implementation of pro-active policies and procedures in relation to information security management, whilst strengthening them with a forensic and incident response capability.

History validates such a strategy when you consider that many organisations are unaware of how readily the information intruder will exploit weaknesses and

---

[40] Clark, Andrew J. (2004). Solicitors Journal. Vol.148 no. 24 Supp (Expert Witness Supplement Summer 2004) pages 14, 16

[41] Chappell, Laura. 'Introduction to Network and Local Forensics.' [Online] http://www.packet-level.com/pdfs/TUT186-Forensics.pdf

[42] Study by Verizon Business Risk Team entitled '2008 Data Breach Investigations Report', recommended the creation of an incident response plan. [Online] http://www.verizonbusiness.com/resources/security/databreachreport.pdf

[43] February 2005 to June 2006 – Hydrasight and Enterprise Management Association (EMA) examined stock prices of companies who had disclosed an information security breach and found that their shares fell by 5% within a month and did not recover pre-incident for nearly a year.

[44] http://www.gocsi.com/press/20050714.jhtml

how easy it is for them to subsequently, sell, trade or use that data for a range of unlawful activities.

> *"Clicking on the above links will lead you to the illicit underworld of the Internet" (Internet.com)*[45]

Despite all current legislation and regulation, as well as organisational adherence to best practice, policy implementation and recognising standards, there is still:

1. A continued growth in criminal data markets
2. An increase in the reluctance to report IT abuse and data compromises
3. A growing risk to reward\punishment ratio for e-crime
4. A challenge for all organisations to keep up with the advances in technology
5. Contrary to the Information Commissioner's stance, data being taken offsite on laptops and other portable devices[46]
6. A failure by organisations to acknowledge that any security breach that leads to data loss is their responsibility.

However, what is likely to further the private sector's ability to investigate IT enabled abuse is the thought of legal sanctions. This will be an increasing motivator that will cause organisations to consider the establishment of electronic management, the implementation of new security principles and the establishment of an e-crime department, because if we do not take action we will fall ever further behind the offender instead of getting as close as possible.

At the same time it is key to acknowledge the advancement already being made, it remains essential that such progress does not remain predictable and that all concerned look to introduce new and innovative measures, for example:

1. Prepare IT systems as a source of evidence by having a forensic capability and prepare staff to be able to respond to hi-tech incidents. At the same time support them with achievable, efficient and effective control policies and procedures.
2. Establish E-Crime Departments to fill the gap between IT Security and General Investigation Departments, or ensure that they have a third party e-crime capability.
3. Regular reviews and practice of security controls so that they keep pace with the growing illegal use of new technologies.
4. Introduce policies and procedures for the collection and seizing of electronic evidence, and these in turn should be incorporated into any incident response policy.
5. Bring in pro-active hi-tech crisis management so as to identify those who use technology for an unlawful purpose, in particular IT abuse and data compromise.
6. Understand the offender and keep up with their techniques through the use of digital intelligence.
7. Make sure that data is effectively protected from loss or theft.
8. Have designated individuals identified who will ultimately take responsibility for the final accountability of any breach of security and\or loss of data.

The implementation of such measures will cause to be put in place a new and positive approach to protecting data and an opportunity to set up an early warning system that will inform us when compromised data is being bought, sold and used for illegal purposes.

[45] Internet.Com, E-commerce. (2002, September 20). The Great Credit Card Bazaar. Retrieved October 18, 2006 from http://www.internetnews.com/ec-news/article.php/1467331

[46] www.ico.gov.uk