2007

Information Security Surveys: A Review of the Methodologies, the Critics and a Pragmatic Approach to their Purposes and Usage.

Alexis Guillot
Edith Cowan University

Sue Kennedy
Edith Cowan University

DOI: 10.4225/75/57b52de0b8754
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

Information Security Surveys: A Review of the Methodologies, the Critics and a Pragmatic Approach to their Purposes and Usage.

Alexis Guillot & Sue Kennedy
School of Computer and Information Science,
Edith Cowan University, Perth, Western Australia
aguillot@student.ecu.edu.au
sue.kennedy@ecu.edu.au

Abstract

Each year the latest information security surveys are released to the computing and business communities. Often their findings and their methodologies are subject to criticism from the information security community, professional bodies and others in the profession. This paper looks at the viewpoints of both the producers and the critics of the surveys. The criticisms cover such issues as the methodologies, the response rates, the experience of the respondents, the design of the questions and the interpretation of the results. This paper looks at these issues and discusses the validity of these criticisms, the impact of the surveys and their value to business and government. It compares the methodologies of some of the largest local and international players in the area. It discusses the issues arising from flawed methodologies, inaccurate information and poor processes, including the perceived lack of integrity and the accuracy of the measurements and methodologies. Despite the strong criticism a middle ground emerged. Data input by the participants, whether accurate or not, may be highly subjective and influenced by their environment and business profile. Furthermore, security at a business level may be extremely complex, the governance principles dictating that the organisation profile, management ideologies and core business values must be accounted for and balanced even for IT. The paper also considers the interpretation of the results and how they may be influenced by current and future products and the vendors of those products. Finally the paper takes a closer look at the use of the surveys in a business context and attempts to show that if constructively used, these surveys can be powerful metric tools used in driving information security strategies in spite of their perceived deficiencies.

Keywords

Information security surveys, methodology, critics, business context, interpretation of results

INTRODUCTION

Each year the latest information security surveys are released to the computing and business communities. This event is usually characterised by frustration and anger throughout the information security profession.

Information Security surveys can be a sensitive topic of discussion with some critics describing them as harmful (Walsh, 2006), whilst most of the others limit the scope of their criticism to the response rates, or lack of, and the managerial reluctance to divulge information (Emergent Chaos, 2006).

This paper will present an overview of some of the more prominent Information Security surveys that are freely available on the Internet. The paper will review and compare their methodologies, target audience and the results of their measurements. The criticisms that they attract from the profession will be analysed in order to highlight the limitations affecting the surveys.

SURVEY SELECTION

Selection methods

Security professionals use the statistics from these surveys for conferences, training and awareness campaigns (Theronsolutions, 2006). Observations, comments, interpretations and analysis of the security surveys have been posted on the Internet, prompting debate within the security community each year (Walsh, 2006).

Before reviewing the surveys it was necessary to reduce the number of surveys reviewed to a manageable and representative selection. The selection of one survey over another can be highly subjective. To overcome this

issue a series of selection criteria were defined and applied to the different surveys. The following criteria were used in selecting the surveys used in this paper:

The survey must:

- be directed specifically at Information Security risk;
- outline statistical measurements of the security items measured:
    - *some surveys are advisory only and are limited to concluding arguments with regards to previously analysed measurements;*
    - *for the purpose of this paper, the survey must include the statistical information;*
- include a justification of the methodology and clearly state the nature of the respondents (eg IT managers);
- have a minimum of three years existence and include in the presentation of the results a comparison to the previous years in order to assess the trends over the recent years;
- be selected from sources representative of current security professionals including, but not limited to, vendors and industry leaders, independently mandated surveys and government reports.
- the surveys must be freely available to the community.

Note: Both international and country specific surveys were considered.

Methodologies

The scope and depth of the information presented by each survey varies, rendering a comparison harder to make.

The methodologies employed by the participants show similarities in the procedures taken to design, collect and review the questionnaires.

In order to maximise the accuracy and fairness of the methodology review the information collection was limited to the following criteria:

- audience surveyed;
- dates and timelines associated with the surveys;
- any available information regarding the design, collection and analysis of the information (i.e.: by whom, collection method, parties involved);
- response rate.

It is important to note that any information transcribed below is directly quoted from the associated survey.

The following five surveys were selected for review.

AusCERT: 2006 Australian Computer Crime and Security Survey:

The Australian High Tech Crime Centre (AHTCC), the Australian Federal Police (AFP), the Police from NSW, QLD, SA, Tasmania, VIC, WA, Northern Territory and AusCERT have collaborated to produce this survey. The survey was funded by the Australian government's Attorney-General's Department and ACNielsen, a market research and information company, was engaged to assist with the preparation and administration of the survey.

The survey was adapted from the 2006 CSI/FBI survey, providing the opportunity to compare Australian findings with the United States in some areas (AusCERT, 2006, p. 37).

- The survey was deployed May 22, 2006
- Respondent answers cover the 12 months period before January 2006.
- Business reply-paid envelopes were sent to 2024 IT managers or their equivalents from a range of Australian public and private sector organizations. Those organizations were invited to complete the survey on-line or return the paper questionnaire via the reply-paid envelope. Responses were also sought from a number of private and public sector industry groups, including the Trusted Information

Sharing Network (TISN), whose members were invited to complete the survey via the secure web site.

- Yielding 389 respondents (17% of response rate).
- All responses were anonymous.
- The acknowledged margin of error was not available. However, readers were warned that the format of the survey changed to increase the survey sample size; this should consequently be considered when assessing the respondent percentages against previous years.

CSO Magazine: E-Crime Watch Survey 2006

The 2006 E-Crime Watch survey was conducted by CSO magazine in cooperation with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Coordination Centre and Microsoft Corporation (CSO, 2006, p. 1).

- The survey was deployed June 28, 2006, through July 30, 2006.
- Respondent answers cover the period between July 2005 and June 2006.
- An e-mail invitation containing a link to the survey was sent to 15,000 CSO magazine readers (CSOs, security and law enforcement professionals);
- Yielding 434 respondents (2.89% of response rate).
- All responses were administered anonymously.
- The acknowledged margin of error is +/- 3.4 percent.

CSI/FBI: Computer Crime and Security Survey

This survey is conducted by the CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad.

Its aim is to raise the level of security awareness, as well as help determine the scope of computer incidents in the United States (U.S.) (CSI/FBI, 2006, p. 1).

- The survey was deployed early January 2006.
- Respondent answers cover the year of 2006.
- Hardcopy (fist-class mailing), and e-mail versions of the survey were distributed to 5000 information security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities.
- Yielding 616 respondents (12.3% of response rate).
- All responses were administered anonymously.
- The acknowledged margin of error was not available.

Deloitte: 2006 Global Security Survey

Deloitte is a private, global audit, tax, consulting, and financial advisory company.

Their Global Security Survey provides benchmarks for IT security in the financial services industry. The goal of this survey is to gather information globally and it encompasses financial institutions with a worldwide presence and with head office operations in the determined geographical regions (Deloitte, 2006, p. 5).

- The survey was deployed June 15, 2006.
- Respondent answers cover the year of 2006.

- Data collection involved collection of both qualitative and quantitative data for related geographical areas. Each participating region was assigned and held accountable for obtaining answers. Most data collection took place through face-to-face interviews with the Chief Information Security Office/Chief Security Officer (CISO/CSO) or designate, or in some instances, the security management team. The option to submit answers online using an online questionnaire was given also.
- 3-activity sectors were surveyed, accounting for 100 global financial institutions, 100 global banks, and 50 global insurance companies.
- This yielded 31 respondents amongst financial institutions surveyed (31% response rate), 34 respondents amongst global banks surveyed (34% response rate), and 16 respondents amongst global insurance companies surveyed (32% response rate)
- Respondents' anonymity was preserved by not identifying their organisations.
- The acknowledged margin of error was not available.

Department of Trade and Industry: *Information Security Breaches Survey* 2006

The Information Security Breaches Survey 2006 is managed by PricewaterhouseCoopers on behalf of the U.K. Department of Trade and Industry (DTI). This biennial survey of U.K. businesses is the U.K.'s leading source of information on security incidents suffered by businesses, both large and small (Department of Trade and Industry, 2006 p. 4).

- The survey was deployed April 25, 2006.
- The sample was randomly picked from a register of U.K. businesses; the contact person being identified as responsible for information security. A total of 1001 computer-assisted telephone interviews were conducted, each lasting on average 30 minutes. In addition, surveys were interactively run at a meeting of the Information Security Forum (ISF), providing an insight into security practices operating in very large businesses. Face-to-face in-depth interviews with information security officers were run, and finally, an e-mail pool was issued to InfoSecurity Europe subscribers. PrincewaterhouseCoopers managed the survey for the DTI and it was sponsored by Microsoft, Clearswift, Entrust and Symantec.
- The number of respondents is unknown; the methodology however leads us to believe that the analysis was performed on a minimum of 1001 respondents, which made up for 100% response rate.
- All responses were administered anonymously.
- DFI acknowledge being 95% confident that the margin of error in their results is no more than +/- 3% percent. In addition, the point is made that with extreme results (towards 0% or 100%) the margin of error is reduced, whilst results analysed for a sub-sample (around +/- 1%) show that the margin of error is greater (large company statistics have a margin of error of no more than +/- 9%). Sampling error, question wording and practical difficulties in conducting surveys can also introduce error or bias into the findings.

Table 1
Summary of the Sponsors, Managers, Participants and Methodologies for the Selected Surveys.

Surveys	AusCERT	CSO	CSI/FBI	Deloitte	DTI
Country surveyed	Australia	U.K.	U.S.	Worldwide	U.K.
Profile	Independent Non-profit	Private	Public association (CSI) / Government (FBI)	Private	Government
Sponsors or cooperation by	**Managed by:** ACNielsen **Sponsored by:** AFP and police from each state force, AHTCC, Attorney-General's Department	**Managed by:** CSO & CERT **Sponsored by:** U.S. Secret Service, Carnegie Mellon University, Microsoft	**Managed by:** Computer Security Institute (CSI) and the computer intrusion squad from San Francisco (FBI)	**Managed by:** Individual Deloitte national headquarters around the world	**Managed by:** PCW **Sponsored by:** Microsoft, Symantec, Entrust, ClearSwift
Frequency	Yearly	Yearly	Yearly	Yearly	Every 2 years
Participants	IT managers or equivalent, TISN members, A number of private and public sector industry groups	CSO readers	Information Security practitioners	CISO CSO Designated Security managers	ISF members and randomly picked U.K. businesses (the preferred contact person was not mentioned)
Sample size	2024 (389 responded)	15 000 (434 responded)	5000 (616 responded)	250 (81 responded)	1001 (1001 responded) + Polls (unknown)
Response rate	17%	2.89%	12.3%	32.4%	> 95%
Survey method	Mail hard-copy and Web-site	E-mail	Mail hard-copy and E-mail	Face-to-face interviews and Web-site	Face-to-face and Phone interviews, E-mail polls

THE CRITICISMS

It is a reasonable assumption that the results of the surveys are only as good as the answers provided by the participants. In a perfect world security metrics would be implemented at every level of the systems and the participants would simply answer the survey questions based on those metrics. Unfortunately, this approach is fundamentally flawed as it relies on the assumption that the participants have in their possession, and are using, appropriate security metrics such as monitoring and audit results to complete the questionnaires. The methodologies did not provide proof that this was the case.

This leads to the question of how do the participants answer the questions and do they have any biases when answering them? The surveys all fall short in addressing those issues.

Furthermore, the scope of the questions goes beyond the technical metrics covered by monitoring and auditing systems. Many surveys now collect information on the financial losses resulting from attacks, the outcomes of reporting the events to law enforcement agencies and, sometimes, the short-term strategies implemented to improve security. For that information to be reflective of the company's profile it is implied that the appropriate person will be answering those questions.

Similarly, some questions attempt to measure the use of certain security technologies and their usefulness in preventing attacks. However, no basis is provided to ensure the proper implementation of those technologies. To illustrate this, 98% of the participants to AusCERT (2006, p. 8) claim to have anti-virus protection in place, yet more than 65% of them detected virus attacks. Does this mean that the remaining 35% experienced successful virus attacks, or did they not detect any attacks? Another factor to consider is the frequency of the virus definition updates which might differ from one organisation to another. The confusion could be due to the

wordiness of the questions, leaving the readers and the respondents unclear as to whether or not the aim is to measure the number of successful attacks, the number of detected attacks or simply the number of attempted attacks.

There is a general lack of information on the methodologies. Walsh (2006) noted that the CSI/FBI 2006 survey response rate was just over 12% and questioned whether "the 12% who did answer differ in any other way from the 88% who did not?" Walsh asked. "We do not know, because the report doesn't tell us".

Ira Winkler (2006) strongly critiqued the CSI/FBI surveys. His arguments all relate to the methodologies and statistical validity of the results. He argues that the term 'attacks' was broadly defined and that there was an implication that the technologies in use were meant to stop the broadly defined attacks.

Winkler comments that "more than 50% of the respondents were from companies with less than $5 million in annual revenue". Those results cannot be statistically generalised to the Fortune 2000 companies, only to companies with less than $5 million in annual revenue.

He also highlights the false perception that security technology is ineffective. Garreston and Messmer (2006) agree with this, tagging the surveys as a great way of creating FUD (fear, uncertainty and doubt): "FUD created by survey results sends the message that you're never secure enough … be afraid, be very afraid". FUD is a sales marketing or political strategy disseminating negative but vague or inaccurate information (CSO Online, 2003).

"Let's face it: surveys for the security industry are created primarily for marketing purposes" (Winkler, 2006). Winkler's statement gained increased credibility when IBM, in their Global Business Security Index, used the CSI/FBI 2005 survey numbers on insider attacks, shortly followed by the announcement of a new fraud detection capability that monitors users' online transactions for questionable activity (IBM, 2006),.

Are the surveys so inaccurate and flawed that they should be rejected as a useful source of information? Winkler (2006) certainly thinks so as he advises his readers to "assure management that it has no valid implications for your business". Whilst the lack of information associated with the surveys' methodologies leads to similar conclusions, should such an opinionated mindset be adopted?

The paper will now consider the surveys and their usefulness to business.

SURVEY PURPOSES: MEASUREMENT TOOLS WITHIN A CONTEXT

Three key reasons were identified as to why the surveys failed to pass the critics' tests:

- People have different notions of what constitutes risk, threat and vulnerability (Ames, 2007).
- The surveys are an indicative measurement of security as it happens in a business context or a health check assessing you against the competition (Deloitte, 2006, p. 4).
- "So far no one has come up with a common, clear, straightforward way of measuring risk that applies or works equally well in all circumstances" (Ames, 2007).

Whilst the definition of risk, threat, and vulnerability may vary from one individual to another, it is imperative to remember that the objectives of the surveys are to "help respondents assess the state of information security within their organization" (Deloitte, 2006, p. 4). This provides a very specific context that needs to be considered when defining the associated risks, threats and vulnerabilities. In turn, the risk profile of those organisations will play an equally important role.

Most of the surveys address those issues. DTI (2006, p. 4) acknowledges that "businesses of different sizes tend to exhibit different security profiles", and has attempted to address this issue by increasing the sample size of the most representative and predominant industry. By boosting the sample of the most representative and predominant industry, in their case sole traders and small SMEs, when the results for a large company significantly differed from the overall results, they were quoted separately.

It is important that the survey questions and results should be interpreted in their intended context. With regard to this context, the surveys can be used as a risk measurement tool, as a justification to support security decision-making and as a marketing argument for vendors.

Risk measuring tool

Measuring risk can be done in two ways; a qualitative one, as outlined by the Australian risk management standards (AS/NZS 4360:2004, 2004) using a model that rates risks as High, Medium, Low and a quantitative one that uses probabilities and statistics to measure losses and risks. The United States General Accounting Office explains that "efforts to develop precisely quantified risks are not cost-effective"; the amount of time and

effort involved in the process are simply too great. (GAO, p. 28). Qualitative measures on the other hand can be developed as a more granular and sophisticated approach. Using risk matrix representation facilitates the representation of the risk gradation levels based on their impacts and likelihood (Amos, 2007).

In a business context, value is determined and represented by a monetary term. Managing risks represents an investment which can be measured. "So we should be able to relate measures of risk to the money we need to manage it" (Ames, 2007).

In this respect every survey contained a measure of the financial gains, loss or value associated with IT Security. Each survey measured the following points:

- Present and future budget allocation towards IT Security;
- Financial expenses related to IT Security controls;
- Investments made towards the improvement of IT Security;
- Financial loss due to the measured incidents.

Some measurements were more technical than others. CSI/FBI (2006) questioned its participants on the Return on Investment (ROI) engendered by IT Security controls. Similarly, Deloitte (2006) and DTI (2006) had questions dedicated to the monetary values associated with the outsourcing of security and insurance expenses.

This is emphasised by the 2007 edition of the CSI/FBI survey which now contains a "business justification" section. "It has generally been believed that projects designed to increase an organization's information security will not automatically be approved by senior management (e.g., by the CFO), but instead need to be justified in economic terms" (CSI/FBI, 2007, p. 8). Those measurements have been in the CSI survey since 2004; however, it is the first year that all economic arguments have been grouped into one section. These include the budgeting and financial management related measurements (loss, investments, cost-benefit measurements), insurance and outsourcing costs.

A decision making tool

KPMG Netherlands (2006, p. 8) argues that Information Systems are at the core of most companies, an integral part of their nervous system.

> It hardly requires explaining that organisations must take effective measures to control the security and continuity risks that come from using information and communication technology … Organisations that have the security and continuity of their systems in place do not need to worry about the risks.

Yet their experience shows that managers and executives often overlook information security, treating it as an isolated phenomenon rather than an integrated part of the business. With regard to those problems it is only logical that some IT managers use these surveys to help loosen the company purse strings to fund security projects. Could it be that the economic measurements included in those surveys are valuable to security despite the criticism? Michael Dean (cited in Garreston & Messmer, 2006), who supports a 50,000 computer network for 175,000 students and teaching staff in Palm Beach County School District Florida, states that he reluctantly support the points many of these surveys are making, "even though some of them make you cringe because they're so blatantly oriented toward selling products".

Jim Hite, supervisor of network services and central operations with Virginia's Prince William County schools (cited in Garreston & Messmer, 2006) explains, "surveys are one of the only benchmarks you can use to make decisions".

A marketing tool

Questionnaire design can be a daunting task (Leedy, 1993; Trochim, 2006). Table 1 showed the existence of partnerships with influential sponsors such as Microsoft, Symantec and other large security vendors. Those relationships, other than being one of the critics' favourite arguments, also seem to indicate the interest and endorsement of those studies by the industry and that they act as a quality improvement factor in some cases. AusCERT (2006, p.3) and DTI (2006, p.4) both provide indicators that such partnerships and industry involvement provided them with larger sample size, more rigour into the survey instrument itself and a more precise question design.

On the other hand, it is only fair to acknowledge that vendors are sponsoring many of those surveys and no one expects to see results that would contradict or negate the need for one of their products. Equally, the surveys are also a tool for vendors to scan the market for guidance. In 2004, Proofpoint, through Forrester Research conducting a survey (Forrester, 2004), found that the results showed that 43% of companies sampled scanned

outbound e-mail for confidentiality breaches. A few months later Proofpoint released an outbound compliance solution that automated the scanning process (Proofpoint, 2005)

Keith Crosley, director of market development with Proofpoint (cited in Garreston & Messmer, 2006), mitigated the critics: "There's always a self-serving aspect to anything a vendor releases … but we really are trying to educate markets and share interesting data that helps people make really intelligent decisions about their technology investments".

However, it is not only the vendors who use the surveys as a marketing tool. IT and Information Security staff can use the results to support their business cases for new security-related systems and products. "As highlighted in the survey, they have to make their case: security professionals are increasingly being asked to develop detailed business cases to justify new investments in technologies they need to address the constantly evolving threat." (CSI/FBI, 2006, p.22).

Interpretation of the Results

The previous section raised the issue of the survey results influencing vendors. However, this is only useful if the interpretation of the results is correct (or if you have a product to sell that addresses the problems identified in the survey). One of the noticeable trends over the past few years is the change in the source of the reported attacks. Until recently the majority of the attacks were reported as coming from the inside, not the outside, of an organisation. Over the last few years this bias has shifted from internal to external. Various explanations are given, such as increased security, increased security awareness, better functioning security measures and the effect of the Sarbannes-Oxley Act, to name a few (CSI/FBI, 2006).

There is another explanation that is rarely mentioned in the analysis of the surveys. There have been two major trends in the states and countries covered by the surveys in the past seven years. The first is the increase in Broadband for home use (Horrigan, 2006). The second is the increase in availability of corporate systems over the Internet and, as a side-effect of this, the increase in employees working from home, often (but not always) using a Virtual Private Network (VPN) to access internal corporate systems. The Office of National Statistics in the UK states that the number of people working from home doubled between 1997 and 2005 (Security Park, 2007). These changes mean that internal staff, contractors and others, now have the opportunity to abuse an organisation's systems remotely rather than when they are at their desks and possibly under scrutiny. The National Threat Assessment Center of the U.S. Secret Service undertook an Insider Threat Study (Capelli et al, 2005) in conjunction with the Software Engineering Institute at Carnegie Mellon University. The findings showed that "30% of the incidents took place at the home of the insider using remote access to the organization's network"; "only 17% of the insider events studied involved individuals with administrator access"; and "87% of the attacks used very simple user commands that didn't require any advanced knowledge". This also was found in other surveys and Kevin Beaver stated in the online Information Security Magazine that "A considerable amount of insider abuse is performed offsite via remote access software". He continued "Simply put, users are less likely to be caught stealing sensitive information when they can it do offsite." What is worrying about this is expressed by Insider Threat Study (Capelli et al, 2005) when they say that "the majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable." Also the fact that "remote access was used to carry out the majority of the attacks" and that these "insider activities caused organizations financial losses, negative impacts to their business operations and damage to their reputations."

These findings could indicate why the percentage of insider attacks has been overtaken by outsider attacks in many of the surveys. In fact it is the classification that is questionable. Should an attack from outside of the organisation physically be classed as an external attack if it is perpetrated by insiders acting remotely? This is further confused if you consider the use of a VPN.

Another problem in trying to analyse the trend from internal to external attacks is that the method of reporting insider and outsider attacks varied not only between the different surveys but also from year to year in the same surveys. Some report the percentage of insider versus outsider attacks; for example, the CSO survey in 2005 reported that 80% of the attacks reported were external and 20% internal; however, in 2006 they reported that 55% of the respondents had reported internal attacks and 58% had reported external attacks. In 2007 the survey question asked who caused more damage, insiders or outsiders? The "results were fairly close (insiders 34%, outsiders 37%, unknown 29%)" (CSO magazine et al, 2007). This makes it harder to use these statistics to recognise trends.

What comes through strongly in the surveys is that the number of incidents has dropped but the cost of those incidents has risen, as illustrated by the title of the 2006 E-Crime Watch Survey Summary, "Survey shows E-crime incidents are declining yet impact is increasing" (E-Crime Watch Survey, 2006).

Again this could be explained if the 'external' attacks were actually being perpetrated by internal personnel who have the knowledge to know what, where and how to attack the organisation so as to gain most benefit. This is a difficult issue as it relates to trust issues with employees, but is also their families (and friends) who may be using the same computer over which the organisation has little control. *Kevin Cheek, vice president of marketing at Reconnex stated that "No one is discussing the risks of remote access because every business routinely gives it to trusted employees, partners, consultants, and other third parties, but businesses really don't know what users are accessing or viewing," (Cheek, 2006). He continued by raising the issue of the need to monitor all SSL or IPSec VPN connections into corporate networks as organisations need to know where their staff are "going and what files they're touching."*

Bruce Schneier (2005) commented on the issues raised in a survey conducted by ICM Research in various European countries. He stated that the results would be equally applicable in the US and probably elsewhere, (such as Australia). The survey found that 21% of workers let family and friends use their PCs to access the Internet, "51% connected their own devices" to them and a quarter of them do it every day. 60% stored personal content on them and 62% "admitted they have a very limited knowledge of IT security". As with some of the other studies a security firm, in this case McAfee, had an interest in the study, however, that should not negate the general findings of the surveys.

CONCLUSION

A mix of local and internationally conducted surveys was reviewed. Some were openly sponsored by vendors, others outsourced to professional survey services. Their methodologies, highly criticised by security professionals, supplied too little information to disprove their detractors. However, over recent years the surveys have been subject to continuous improvement. Recent changes included more business-oriented metrics applied to risk measurement and the search for larger and more appropriate samples. Further improvements are coming from the Deloitte and DTI surveys, which outline comprehensive methodologies, a closer focus to certain industries and in-person interviews.

Winkler (2006) argued that management should be reassured that survey results have no valid implications for their business. Others question the interpretation of the results and their implications for business and government. Overall it would be preferable to think that security professionals are able to use the findings from the surveys for the good of security within their organisation regardless of these criticisms. This includes valuing security improvements primarily by leveraging the existing tools to their advantage, including information security surveys. This is good practice and, if applied well, can be a powerful driver for both business and its information security. This is none other than good Governance through risk management, performance evaluation and even strategic alignment by benchmarking your company's results against a global scale.

REFERENCES

AS/NZS 4360:2004. (2004). AS/NZS 4360:2004: Risk management. NZ: Standards New Zealand.

AusCERT. (2006). 2006 Australian Computer Crime and Security Survey. Retrieved September 15, 2007, from http://www.auscert.org.au/images/ACCSS2006.pdf

Brenner, B. (2006). Has CSI/FBI survey jumped the shark? Retrieved September 15, 2007, from http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1202328,00.html

Beaver, K. (2005). Five common insider threats and how to mitigate them. Retrieved October 10th, 2007.

http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1158172,00.html

Capelli, D., Keeney, M., Kowalksi, E., Moore, A., Rogers, R. , Shimeall, T. & et al. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. National Threat Assessment Center, United States Secret Service, Washington, DC & CERT® Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. Retrieved October 11, 2007. http://www.cert.org/insider_threat/insidercross.html

Cheek, K. (2006). Reconnex Insider Threat Index Reveals Use of Remote Access and Rogue VOIP Protocols, Exposure of Confidential Information. Retrieved October 10, 2007, from http://www.reconnex.net/news_events/pr/pr_05.01.06B.php

CSI/FBI. (2006). Computer Crime and Security Survey. Retrieved September 15, 2007, from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

CSO magazine, U.S, Secret Service, CERT Program, Microsoft Corp. (2007). 2007E-Crime Watch Survey – Survey Results. Retrieved October 10th, 2007 from http://www.cert.org/insider_threat/

CSO Online. (2006). Glossary: Fear, Uncertainty, and Doubt (FUD). Retrieved September 20, 2007, from http://www.csoonline.com/glossary/term.cfm?ID=1223

CSO. (2006). E-Crime Watch Survey 2006. Retrieved September 15, 2007, from http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

Deloitte. (2006). 2006 Global Security Survey. Retrieved September 15, 2007, from http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006%20Global%20Security%20Survey_2006-06-13.pdf

Department of Trade and Industry. (2006). Information Security Breaches Survey 2006. Retrieved September 15, 2007, from http://www.pwc.com/U.K./eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf

Emergent Chaos. (2006). What Me Data Share? Retrieved September 15, 2007, from http://www.emergentchaos.com/archives/2006/07/what_me_data_share.html

Eppel, N. (n.d.). Security Absurdity: The Complete, Unquestionable, And Total Failure of Information Security. Retrieved September 16, 2007, from http://www.securityabsurdity.com/failure.php

GAO. (1998). Executive Guide: Information Security Management. Retrieved September 16, 2007, from http://www.gao.gov/archive/1998/ai98068.pdf.

Garreston, C. & Messmer, E. (2006, March 20). It's raining IT security surveys. Retrieved September 19, 2007, from http://www.networkworld.com/news/2006/032006-security-surveys.html

Horrigan, J.B. (2006). Home Broadband Adoption 2006. Pew Internet & American Life Project. Retrieved October 11th, 2007. http://www.pewinternet.org/pdfs/PIP_Broadband_trends2006.pdf

IBM. (2006). IBM Unveils New Solution to Eliminate Insider Attacks. Retrieved September 19, 2007, http://www-03.ibm.com/press/us/en/pressrelease/19268.wss

KPMG Barbardos. (2006). Information Security Survey 2006. Retrieved September 15, 2007, from http://www.kpmg.bb/news.asp?unid=55

KPMG Netherlands. (2006). Information Risk Management: Information Security Survey, Six important signals. Retrieved September 15, 2007, from http://www.clubofamsterdam.com/contentarticles/27%20Electronic%20Identity/information%20security%20survey.pdf

Landesman, M. (2006). Chase Online Reward Survey. Retrieved September 19, 2007, from http://antivirus.about.com/od/emailscams/a/chase.htm

Theronsolutions. (2006, July 17). The CSI/FBI 2006 Survey Considered Irrelevant. Retrieved September 15, 2007, from http://theron.com.my/blog/2006/07/17/the-csifbi-2006-survey-considered-irrelevant/

Trochim, W.M.K. (2006, November 10). Survey Research: Constructing the Survey. Retrieved September 19, 2007, from http://www.socialresearchmethods.net/kb/survwrit.php

Leedy, P. D. (1993). Practical research: planning and design. (5th ed.). New York: Macmillan.

Proofpoint. (2005). Outbound Email Security and Content Compliance in Today's Enterprise. Retrieved September 19, 2007, from http://www.suremessage.co.uk/whitepapers/Proofpoint_Outbound_Email_Security_and_Content_Compliance_2005.pdf

Schneier, B. (2005, December). Insider Threat Statistics. Retrieved September 19, 2007, from http://www.schneier.com/blog/archives/2005/12/insider_threat.html

Security Park (2007). SafeMove eliminates Wi-Fi hotspots security threats. Retrieved October 11, 2007. http://www.securitypark.co.uk/security_article259965.html

Walsh, C. (2006). CSI/FBI Survey considered harmful. Retrieved September 15, 2007, from http://www.emergentchaos.com/archives/2006/07/csifbi_survey_considered.html

Wilson, T. (2006). CSI/FBI: Small Firms Pay Big For Security. Retrieved September 20, 2007, from http://www.darkreading.com/document.asp?doc_id=97818

Winkler, I. (2006). Opinion: Investigating the FBI's 'invalid' security survey. Retrieved September 20, 2007, from http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1159992,00.html

COPYRIGHT