THE USE, MISUSE, AND ABUSE OF STATISTICS IN INFORMATION SECURITY RESEARCH

Julie J.C.H. Ryan, D.Sc., The George Washington University
Theresa I. Jefferson, D.Sc. The George Washington University

Abstract

Survey data on information security trends and concerns are used to justify increased expenditures on security tools and technologies. Students use the data to support term paper analyses. Government officials use these data to justify program initiatives and to berate companies for inadequate security. The numbers, however, are anecdotal, are not generalizable to the business level, and are reported in cumulative form. In a word, they are not useful for any of the purposes listed above. This paper examines this phenomenon, looking at survey data that has been published and the uses to which it has been put.

Introduction

In order for managers to know how to allocate scarce resources for information security in an environment, it is important to understand where the greatest likelihood for problems lie, how much damage can result from any particular attack or problem, and what benefit accrues from any particular technology or control. Managers need to be able to justify expenditures, through showing an avoidance of costly jeopardy, return on investment, or other managerial tools used to make rational decisions regarding enterprise resource allocations. These calculations must be driven by data that provide such things as the probability distributions of events, the expected loss from certain problems. The collection of data from the world at large can provide that kind of data for savvy managers to then use to assist in the difficult decision process of where to invest scarce resources.

Many research efforts purport to provide that data to managers. A small sampling of recent headlines include the following:

- "Cyber-Attack Costs Down, Says Survey" (Fisher, 2003)
- "Business Not Prepared for E-Risks" (Computer Security Update, May 2003)
- "The Sad And Increasingly Deplorable State Of Internet Security" (Piscitello and Kent, 2003)

The data presented in these articles is sobering and thought provoking. Piscitello and Kent warn that "the security incident rate is doubling annually." (Piscitello and Kent, 2003). The Computer Security Update article on E-Risks states that "19% of employers have battled lawsuits stemming from e-mail/Internet abuse, 31% have experienced loss of confidential information/intellectual property via e-mail, and 35% have terminated employees for e-mail/internet abuse." (Computer Security Update, May 2003) Fisher reports some encouraging news, on the other hand: "The 530 organizations surveyed reported $201.8 million in losses this year; in 2002, 503 respondents lost $455.8 million." (Fisher, 2003) Responsible managers reading these and other articles would certainly have a lot to think about in terms of their enterprises' approaches to security and protection of intellectual assets.

What is lost in the stories of these various research efforts is the nuances and subtleties of the research methodologies used, the statistics applied, and the data reported. An in-depth study of survey data revealed a serious problem in all three of these areas. In many cases, the research methodologies were not sound (in some cases, the results were specifically identified as being unscientific). The statistical analyses were in some cases inappropriate and in general only partial results reported in the press (as might be expected).

While these problems are not unexpected, there is a larger problem that the data is being taken from the popular press and used by policy and decision makers to guide resource allocations in security training, development, and technology applications. There is no doubt that security is of grave concern to the nation and to the business sector. The fact that the data driving the decision processes is in general fundamentally flawed in one or more of the phases of creation, manipulation and reporting is therefore of critical concern.

The Surveys

An analysis was performed on fourteen publicly available surveys on the state of information security practices and experience by business. The surveys chosen represented the most widely publicized surveys within a five year time period of 1995 to 2000. The surveys analyzed are shown in Exhibit 1.

The majority of these surveys targeted information technology professionals and information security professionals at large companies through professional mailing lists or other professional contact databases. Half of the surveys were limited to the North American continent: four of the surveys covered only US firms and three covered firms in the US and Canada. Of the remaining seven, five were global in reach.

Exhibit 1. Surveys Reviewed for Methodology and Results.

Survey	Number Of …		
Name	Respondents	Companies	Countries
NCC Business Information Security Survey 1998 (BISS98)	??	??	UK
Colin Germain/City University of London 1997 Security Survey (CG97)	56	56	UK, Int'l
Issues and Trends: 1997 CSI/FBI Computer Crime and Security Survey (CSI97)	520	??	US
Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey (CSI98)	520	??	US
Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey (CSI99)	521	??	US
Third Annual E&Y Information Security Survey (E&Y95)	1290	??	US, Canada
Fourth Annual E&Y Information Security Survey (E&Y96)	1320	??	US, Canada
Fifth Annual E&Y Information Security Survey (E&Y97)	3599	??	24 global
Second Annual E&Y Global Information Security Survey (E&Y98)	4300	??	35 global
Securing the E-Business 1999 Security Survey (Ebiz99)	1130	??	US, UK, Asia
ISM 1999 Security Survey (ISM99)	745	??	US, Canada
KPMG National Computer Security Survey 1996 (KPMG96)	1452	1452	UK, Ireland
1998 InformationWeek/PWC Global Information Security Survey (PWC98)	1600	??	50 global
Information Systems Security Survey (WarRoom96)	205	205	US

(NCC 1998, Germain 1997, CSI 1997 – 1998, Panettieri 1995, Status of Defense 1996, How We Got Number 1997, E&Y 1998, Securing E-Business 1999, ISM 1999, KPMG 1996, PWC 1998, WarRoom 1996)

The data represented by these surveys must be considered in light of how the data was collected. The surveys predominantly targeted individuals rather than corporations. Only two of the fourteen attempted to specify one response per company. Because the others did not so distinguish, the data can not be generalized to company experiences but only to individual experiences. For the majority of these surveys, it is possible and even probable that responses were received from individuals working for the same company. Therefore, any bit of data must be considered in light of an individual's experiences rather than the experiences of a company. It can not, for example, be said based on this data that a certain percentage of corporations have security policies. It can only be said that a certain percentage of individuals are likely to have security policies in their companies.

Of the fourteen surveys listed, nine, or 64.2 %, solicited responses from information technology or information security professionals. The other five targeted executive managers. Three of the fourteen were targeted solely at large companies. Three of the fourteen collected data from respondents over the Internet.

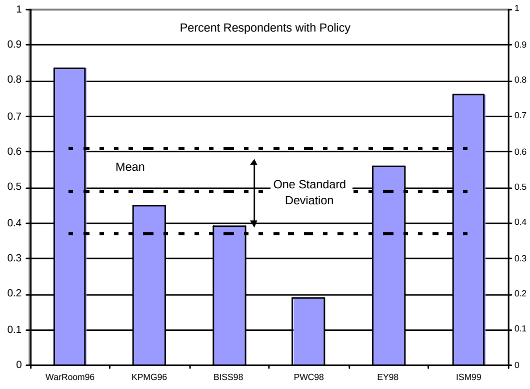
Performing a meta-analysis of the surveys would be difficult because the questions differ both in content and method from survey to survey and because the results were developed and reported in different ways. However, comparing the surveys' common results reveals an interesting divergence of results. For example, seven of the surveys asked the respondents if their organizations had a security policy. The reported results range from 19 % of the respondents as having a policy (PWC 1998) to the "vast majority" of respondents having a policy (Securing E-Business 1999).

Exhibit 2. Percent Reporting Having a Security Policy.

Survey	Those With Security Policy
WarRoom 96	83.4 %
KPMG96	45 %
BISS98	39 %
PWC98	19 %
E&Y98	56 %
ISM99	76 %
Ebiz99	"vast majority"

(WarRoom 1996, KPMG 1996, NCC 1998, PWC 1998, E&Y 1998, ISM 1999, Securing E-Business 1999)

Exhibit 3. Percent Reporting Having a Security Policy with Mean Plotted.



In chronological order, the survey results regarding the existence of a security policy are presented in Exhibit 2. Even within specific years, the numbers range dramatically. Exhibit 3 shows the data graphically. The grouped data mean and standard deviation, 0.49 and 0.239 respectively, are plotted on the chart. Three of the surveys reported results that fall within one standard deviation of the grouped data mean.

Five of the surveys asked specifically if the respondents had experienced any security breaches in the previous year. The other surveys did not report the aggregate percentage of respondents reporting security breaches, preferring instead to report specific kinds of security incidents.

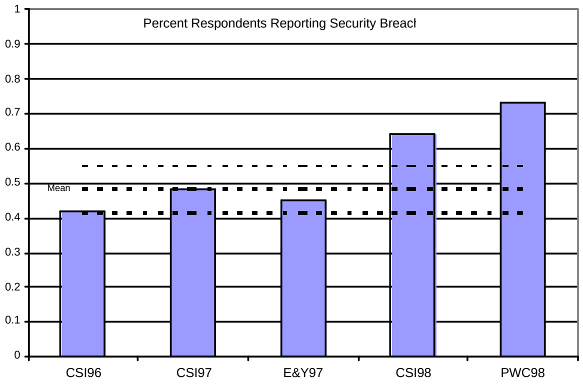
Of the five surveys that did report aggregate percentages of respondents affirming one or more security breaches, the numbers ranged from a low of 42 % (CSI 1996) to a high of 73 % (PWC 1998). Exhibit 4 shows the specific survey data. Exhibit 5 shows the data graphically. The grouped data mean and standard deviation, 0.48 and 0.134 respectively, are plotted on the chart.

Exhibit 4. Respondents Reporting Security Breaches in Previous Year.

Survey	Security Breach in Previous Year
CSI96	42 %
CSI97	48 %
E&Y97	45 %
CSI98	64 %
PWC98	73 %

(CSI 1996, CSI 1997, How We Got Number 1997, CSI 1998, PWC 1998)

Exhibit 5. Respondents Reporting Security Breaches in Previous Year With Mean Plotted.



Examined chronologically, this data would seem to indicate a steady increase in security breaches being experienced. Three of the five survey results fall within one standard deviation of the grouped data mean. Two, CSI98 and PWC98, are well out of range on the high side, reporting 64 % and 73 % respectively of respondents indicating that they had experienced a security breach in the previous year.

Another frequently asked question, covered by nine of the surveys, related to monetary loss resulting from information security failures. Exhibit 6 shows the surveyed results.

As can be seen by the reported data, the ability or the willingness of the respondents to quantify losses is limited at best. In many of the surveys, respondents were willing to admit that they had experienced loss but were unwilling or unable to quantify the losses. Most of the nine surveys approached this area of questioning from the point of view of how much damage had been done in aggregate.

Exhibit 6. Reported Financial Losses Due to Security Problems or Attacks.

Survey	Amount of Loss Reported		
E&Y95	20 % of respondents had losses greater than $1 Mil		
WarRoom 96	Insider	Outsider	
	Unknown	12.7 %	21.0 %
	< $10K	6.9 %	4.4 %
	$10K – 200K	33.6 %	22.9 %
	$200K – 1 M	31.2 %	34.1 %
	> $ 1 M	15.6 %	17.6 %
CSI97	Total losses for the 48 % able to quantify: $100,115,555		
CSI98	Total losses for the 46 % able to quantify: $136,822,000		
BISS98	Average cost for a security breach (all sites): £ 7,146 Average cost per breach, sites over 200 employees: £ 20,199		
PWC98	Of the 82 % reporting losses, 33 % able to quantify losses: -- 84 % lost between $1,000 and $100,000 -- 16 % lost more than $100,000		
ISM99	Total losses reported were $23,323,000 Average loss reported was $256,000		
CSI99	Total losses for the 31 % able to quantify: $123,779,000 Total losses for the 4.4 % reporting theft of proprietary data: $42,496,000 Total losses for the 5 % reporting financial fraud: $39,703,000		
Ebiz99	Average cost for a power related incident: $2,000 Average cost for a virus related incident: $800 Average cost for an email related incident: $500		

(Panettieri 1995, WarRoom 1996, CSI 1997, CSI 1998, NCC 1998, PWC 1998, ISM 1999, CSI 1999, Securing E-Business 1999)

As a result, the losses reported include an average loss cited of $800 for a virus related security incident (Securing E-Business 1999), average costs for a security breach of any kind cited at £ 7,146 (approximately $10,000) (NCC 1998) and $256,000 (ISM 1999), as well as total losses for the year ranging from $23, 323,000 (ISM 1999) to $123,779,000 (CSI 1999).

Eight of the surveys asked respondents about unauthorized access to their systems. Some of the surveys differentiated between outsider access and insider abuse, with some even specifying the kind of insider (employee, contract worker, or business partner). The reported rates show an astonishing range of values, with two surveys showing only 4 % (E&Y 1998) and 8 % (Securing E-Business 1999) of respondents reporting external attacks while other surveys showed as high as 58 % (WarRoom 1996) of respondents reporting outsiders as having attempted to gain access. Of the respondents reporting insider problems, the numbers were much closer together, but still ranging from a low of 44 % (CSI 1998) to a high of 62.9 % (WarRoom 1996). Exhibit 7 presents the comparative data for the eight surveys.

Exhibit 7. Respondents Reporting Unauthorized Access.

Survey	Unauthorized Access
E&Y95	20 % reported actual or attempted network intrusions
WarRoom96	62.9 % caught insiders misusing systems 58 % had outsiders attempt to gain access
CSI98	44 % reported unauthorized access by employees 24 % reported system penetration from outside
PWC98	58 % said that insiders have abused access privileges 24 % have seen outsiders break in
E&Y98	4 % said that they had been broken into 77 % said they had not experienced any break-ins
CSI99	55 % reported unauthorized access by insiders 30 % reported intrusions by outsiders
ISM99	52 % reported employee access abuse 23 reported unauthorized access by outsiders
Ebiz99	8 % reported experiencing attacks from the web

(Panettieri 1995, WarRoom 1996, CSI 1998, PWC 1998, E&Y 1998, CSI 1999, ISM 1999, Securing E-Business 1999)

The data reported for insiders abusing access is shown graphically in Exhibit 8. The grouped data mean and standard deviation, 0.545 and 0.07 respectively, are plotted on the chart. Three of the surveys reported data that falls within one standard deviation of the grouped data mean. The data reported by the other two surveys is in the third standard deviation from the grouped data mean.

Exhibit 9 shows the reported data regarding unauthorized access by outsiders graphically. The grouped data mean and standard deviation, 0.128 and 0.179 respectively, are plotted on the chart. Two of the surveys reported data that falls within one standard deviation of the grouped data mean. Of the six other surveys, five reported data that falls well within two standard deviations while one, the WarRoom 1996 Survey, reported data that lies in the fifth standard deviation (the value for five standard deviations above the mean is 0.576, while the WarRoom 1996 Survey reported 58 % of respondents had experienced outsiders attempting to gain access).

Exhibit 8. Percent Respondents Reporting Insider Access Abuse.

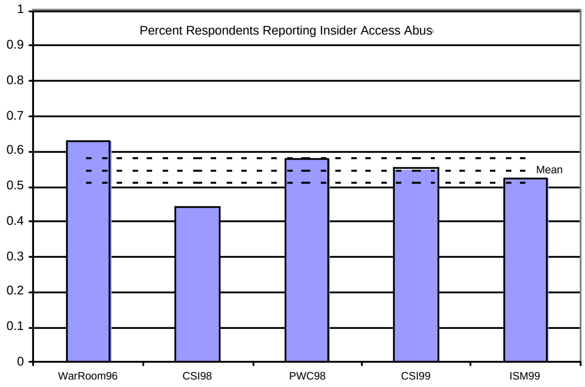
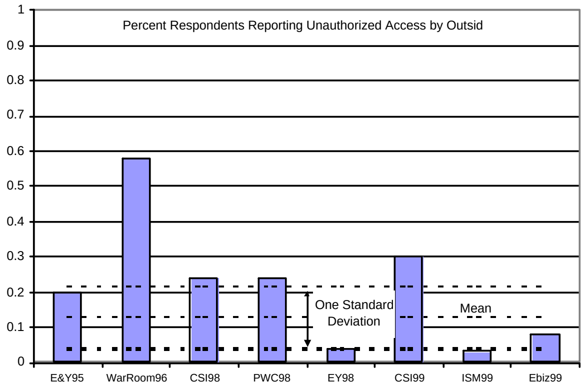


Exhibit 9. Percent Respondents Reporting Outsider Access Abuse.



Seven of the surveys specifically asked about Internet connectivity and security considerations. Again the surveys approached the question from a variety of perspectives, thereby making direct comparisons difficult or impossible. One asked whether the respondents believed it was possible to have secure transactions over the Internet (Germain 1997). Two others asked about general concern about Internet security (Panettieri 1995, Securing E-Business 1999). The others asked if the respondent's Internet connection was a frequent point of attack (CSI 1997 – 1999). The reported results are listed in Exhibit 10.

Six of the surveys asked respondents about how important security was in their organization. On each of the six surveys, the majority of respondents said that security was important. Exhibit 11 presents the data from the six surveys.

Exhibit 10. Reported Concerns with Connectivity.

Survey	Internet Concerns
E&Y95	40 % were not satisfied with Internet security 28 % were satisfied with Internet security 32 % were not sure
CSI96	37 % said Internet connection a frequent point of attack
CSI97	47 % said Internet connection a frequent point of attack
CG97	52 % said it was possible to have secure transactions over the Internet
CSI98	54 % said Internet connection a frequent point of attack
CSI99	57 % said Internet connection a frequent point of attack
Ebiz99	35 % said they are concerned about attacks from the web 8 % said they have experienced such attacks

(Panettieri 1995, CSI 1997, Germain 1997, CSI 1998, CSI 1999, Securing E-Business 1999)

Exhibit 11. Reported Importance of Security.

Survey	Importance of Security
E&Y95	63 % said security as important
E&Y97	84 % said security was important
E&Y98	58 % said security was important
BISS98	72 % rated security as very important
PWC98	56 % said security was a high priority
ISM99	65 % said security had high visibility 83 % said management supports security needs

(Panettieri 1995, How We Got Number 1997, E&Y 1998, NCC 1998, PWC 1998, ISM 1999)

Exhibit 12. Reported Importance of Security with Mean Plotted.

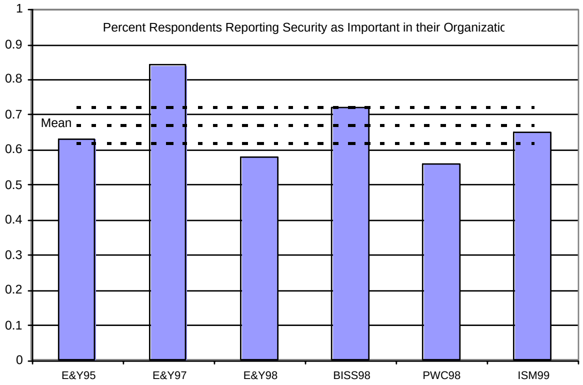


Exhibit 12 shows the data on security importance graphically. The grouped data mean and standard deviation, 0.669 and 0.103 respectively, are plotted on the chart. Of the six surveys, three reported data falling within one standard deviation of the grouped data mean. Two of the surveys reported data falling into the second standard deviation from the grouped data mean and the third, Ernst & Young 1997 Survey, was in the third standard deviation from the grouped data mean.

Eight of the surveys asked respondents what their most important security concerns were. These concerns were solicited in a variety of manners, including asking what the single most pressing concern was (ISM 1999) and asking what the top five security breaches were (NCC 1998). Additionally, the surveys tended to give a set of security breach possibilities for the respondents to choose from, thereby framing the answer space. The top concerns were viruses, some variety of theft (ranging from data to monetary assets), and system component failure, all of which appear in almost all the top five rankings.

Only two of the surveys asked if the respondents' organizations had a business continuity plan or incident response team. The questions were somewhat different, one asking how effective the business continuity plan was in recovering from a breach while the other asked if a business continuity plan had been developed in the previous twelve months, so again the results are not comparable. Coincidentally, both surveys asking this question were both administered in 1998. (NCC 1998, E&Y 1998)

Voodoo Infosec

Scientists and researchers recognize the traps that lie in poorly designed and executed research efforts. A classic text on the subject, "How to Lie With Statistics," provides numerous examples of how statistical data can be used, misused, and abused (Huff 1954). It is critical in all research that close attention be paid to the design and execution of the research so that the data that results will have meaning and be useful. This principle is particularly important in survey based research.

First and foremost of the pitfalls that concern the researcher is the design of the questionnaire. Recognizing that each questionnaire contains only a small sample of all possible questions covering the topic being researched, the questions chosen to be included in the questionnaire must be carefully crafted and structured. The answers that are possible must also warrant close attention. For example, the question, "How many times per week do you eat breakfast?" must include the option of "zero". Omitting that answer possibility potentially biases the results.

Another pitfall lies in the selection of the respondents. Identifying and quantifying the population of interest is a particular challenge, but getting a statistically valid sample from that population can be time consuming and expensive. A true random sample, in which every person or thing in the population has an equal chance of being chosen, is the preferred way to get data in which a researcher can have confidence. A more economical way is the stratified random sample, in which groups within the population are identified and samples designed in proportion to the prevalence within the population. Two problems lie in using the stratified random sample: first, that the prevalence rate is correct, and second, how to handle people who fall into more than one group. These challenges must be addressed in the research design and potential biases be both controlled for and identified clearly.

Finally, it must be recognized that the answers given to a survey may not be correct or true. From a purely philosophical point of view, the answers given represent a sample of the respondent's life experiences and attitudes, which may be influenced by mood, health or whim. But more importantly, the desire of a respondent to give a "correct" answer can cause the respondent to outright lie in his or her response. This phenomenon can be controlled through survey design techniques, but definitely must be considered a priori, particularly when the subject matter is emotional or subject to perceived peer pressure.

The studied surveys that purport to provide research data failed in one or more of these categories, bringing into question the results reported.

Methodology and Design. Many design errors were noted in the fourteen surveys studied. These design errors included the selection of the target sample of the population, the design of the questions, and the methodology of the survey administration.

The respondents chosen to participate in the fourteen surveys tended to be information security professionals in high technology companies. This selection introduces a strong bias in the results for several different reasons. First, the mood in the information security profession during the time period of the survey administration was one of dedicated importance in the face of overwhelming odds, including lack of respect from business leaders and management. It was common during this time frame to hear security professionals complaining about lack of investment in security technologies and training, and of the difficulties in getting upper management to understand that security was not a cost-side ledger entry. This social situation greatly increased the potential for the chosen respondents to inflate their responses on security incidents and experiences. Even without this social pressure, however, there would have been pressure to inflate responses. Whenever a professional is asked about the need for or importance of his/her profession, the tendency is to defend the importance of the profession by exaggerating skills or responsibility.

In several of the surveys, the respondents chosen to participate came from professional association mailing lists. When used year after year, a learning bias was introduced into the results. Thus, a respondent, upon receipt of the latest survey, may mentally think that if he or she answered "two" the previous year, the answer for this year needed to be at least "two" and more probably higher. Additionally, having answered the questionnaire the year prior, the respondent would have been on heightened alert for the elements on the survey to occur in his or her environment. Elements that might have been ignored previously (or simply not come to the person's attention) would gain prominence and importance in that person's worldview.

In most of the surveys, many respondents from the same organization were chosen as part of the targeted population. What might have been a single virus incident, therefore, might have been reported many times, inflating the true incident rate of the problem. Financial losses may have been reported several times, adding up to multiples of the true financial loss.

Reported Results. The publicized results from these surveys were generally limited to descriptive statistics, but inferences tended to be extrapolated from those descriptive statistics. Unfortunately, the corresponding inferential statistics were rarely reported, leading one to wonder about alpha sizes and the normality of the data distribution.

Because the surveys were focused predominantly on individual experiences rather than on business experiences, the results in general could only be attributed at the respondent level, but when reported in the print media were presented as the experiences and concerns at the business level. The implication, therefore, was that a business was likely to experience a certain amount of financial loss or a certain number of security incidents, where the true number was some fraction of those reported numbers.

The surveys relied heavily on reported averages, such as in 'average cost per site'. As any researcher knows, that could be one of three numbers: the arithmetic mean, the median, or the mode. Reading the results as printed reveals nothing about which average the results represent, which leads to the inevitable question of what the data might mean. If the number reported was the arithmetic mean, what was the distribution and the variance? If it was the median or the mode, other questions present themselves. But without even knowing which average is being reported, it is hard to even know which questions to ask.

The Use of the Surveys

The results were reported widely, often in press releases to the public media. The press releases often carried only the most interesting of the data, without much explanation of what the data generally meant.

The stories were picked up and promulgated widely throughout the information security community, by means of internet mailing lists and web-based publishing. As a result of this promulgation, the data gained wide currency as being true and accurate representation of the state of information security. As an indicator of how widely quoted the data is, a simple search on Google (http://www.google.com) using the search term "CSI/FBI survey" results in 4,900 hits. Even in the internet age, that represents a very large promulgation of the data. The websites include the following:

- "Computer Security Facts and Statistics from Harris Corporation" located at http://www.bigwave.ca/~cda/trivia.html;
- "Security Statistics" located at http://www.microsaver.com/tips/tip_1028.html; and
- "The Institute of Management Consultancy (IMC) Special Interest Group for Interim Managers White Paper on Security Information Assets" located at http://www.executivesonline.co.uk/info/papers/imc-rajan-security-paper.pdf.

All of these sources presented the data uncritically as fact, with no interpretation or caveat. None of the sites checked included the caveat that the CSI/FBI survey was conducted in an unscientific basis.

So the question arises: are managers using the data to inform them on how to allocate resources? No research has been done on that question, and it would be a very interesting research program to execute. Anecdotal evidence can be gleaned, however, from two sources: student term papers and government policy documents and testimony.

Student Term Papers. Students who are studying information security and who write term papers that call on the statistics published through such survey reports as the CSI/FBI efforts are those who intend to or who are already working in the field, and who may at some point in time be called upon to manage security efforts for an enterprise. One website that publishes student papers related to information security is the SANS website (http://www.sans.org). SANS is an organization dedicated to educating and training information security professionals. Part of their efforts include certification programs, part of which includes writing one or more research papers. The research papers are posted on the SANS website in the Reading Room (http://www.sans.org/rr/). A search on the SANS Infosec Reading Room website using the search term "CSI/FBI survey" revealed 17 papers that cited the CSI/FBI survey data.

Are the students who are using the survey data examining the data critically and using the data carefully? After all, the CSI/FBI survey readily reveals that it is a non-scientific survey. In fact, none of the 17 papers challenges the data critically and most cite it as fact with no interpretation. To illustrate, several extracts are presented here. The first is from a paper entitled "Security Awareness Training Quiz - Finding the WEAKEST Link" which is aimed at the management challenges associated with controlling security issues:

> The Computer Security Institute recently published the 2001 CSI/FBI Computer Crime and Security Survey and it contained some very interesting statistics:
> -- Ninety-one percent of surveyed organizations detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems). Only 79% detected net abuse in 2000.
> -- Ninety-four percent detected computer viruses (only 85% detected them in 2000).
> Just in these two findings, companies must realize that they need to do everything they can to not only require security awareness training but also require the testing of those employees to determine if they have actually retained the information they were taught and to MAKE SURE they have a basic understanding of information security.
>
> (Sustaita 2001)

The second extract is from a paper describing how to use qualitative risk assessment to assist in management efforts to decide how to control security problems in a measured and structured way:

> A well prepared and experienced reviewer may also use the rapid risk assessment, in which the threat and vulnerability levels are inputted directly into the system with a rating guide (e.g. “very low” threat for an incident “expected to occur on average no more than once in every 10 years”, or “medium” vulnerability for an incident “occuring with a 33% to 66% chance of the worst case scenario realized”) overruling the results from questionnaires. The qualitative approach here may currently be the only choice, since standards and relevant, reliable statistics on threats (except few surveys like annual CSI/FBI Computer Crime and Security Survey [CSI01]) or vulnerabilities are not available to produce accurate estimates on the regularity of them.
>
> (Yazar 2002)

The third and final extract is from a paper describing how to perform mathematical quantitative risk analysis for information security management purposes:

> According to the FBI/CSI 2002 study, even though 89% of the companies surveyed have firewalls and 60% use intrusion detection systems (IDS), an alarming 40% of those surveyed still detected intrusion from the outside (Computer Security Institute). …
> The CSI/FBI 2002 Computer Crime & Security Survey contains several charts useful for calculating the ARO [annualized rate of occurrence] for internet related attacks (Computer Security Institute).
> (Tan 2002)

The clear message here is that students are simply consuming the data at face value without either understanding what it means or questioning the underlying methodology. Further, they are using the data to drive specific methodologies, such as qualitative and quantitative risk assessments.

Government Policy and Testimony. The General Accounting Office (GAO) is responsible for auditing and informing the activities of the 24 Federal Agencies, including their computer security efforts. In order to determine whether the flawed statistics are informing government policy, a search was conducted on the GAO website (http://www.gao.gov). Searching on the term "csi/fbi" resulted in four documents being returned. The oldest document was produced in 1998 while the newest was produced in 2001. The documents included the following:

- "Management Planning Guide for Information Systems Security Auditing" (GAO/NSAA 2001);
- "GAO Report to the Chairman, Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives: Information Security Serious and Widespread Weaknesses Persist at Federal Agencies" (GAO 2000);
- "GAO Report to the Committee on Government Affairs, U.S. Senate: Information Security Serious Weaknesses Place Critical Federal Operations and Assets at Risk" (GAO 1998); and
- "GAO Report to the Chairman, Special Committee on the Year 2000 Technology Problem, U.S. Senate: Critical Infrastructure Protection Comprehensive Strategy Can Draw on Year 2000 Experiences" (GAO 1999).

These documents are clearly influential on national policy at the highest level -- informing the Congress of the United States on issues associated with information security challenges and concerns. Reviewing the documents reveals that the GAO treats the data exactly the same way that the students writing research papers treat the data: as fact, with no questioning of method or meaning. The data is simply presented as statements of fact, from the experts to the decision makers.

Conclusions

Managers owe a duty to those that rely on them: the shareholders, the employees, the clients, the business partners. The duty is to make the best possible decisions regarding use of scarce resources. No manager has perfect information, which makes the challenge of decision making difficult and complex. Thus a manager needs to have the best possible data on which to base decisions.

In the information security arena, there is no reliable data upon which to base decisions. Unfortunately, there is unreliable data that is masquerading as reliable data. The people using that data appear not to question the reliability of the data, but simply quote it with no caveats or constraints. This is of great concern because it may mean that resources are being allocated inappropriately or ineffectively.

There are two conclusions that are drawn from this situation. First, somehow the appreciation for statistics has been eliminated or trivialized in the education process, so there are a great many people who would not know reliable data from unreliable data without having someone explain it to them. These people include not only the journalists who report the data in the popular media, but also managers and security experts who rely on data to inform their decisions. Secondly, there is a strong need for reliable data. The challenge of managing any complex situation requires data that can be used to develop better decisions. This is certainly true in the management of information security architectures and resources.

References

"How We Got The Numbers", InformationWeek Online News in Review, 8 September 1997. http://www.iweek.com/647/47iunum.htm, accessed 4 October 1999.

"Information Security Survey Launched", Rediff On The Net, 25 January 1999. http://www.rediff.com/computer/1999/jan/25kpmg.htm, accessed 4 October 1999.

"Information Security Survey", KoreaLink InfoTech. 26 February 1999. http://www.dailysports.co.kr/14_5/199902/t4551112.htm, accessed 4 October 1999.

"Internet Security Concerns", 2 November 1997. http://multiplex.com/GreensheetIssues/971102-/971102-11.html, accessed 4 October 1999.

"PricewaterhouseCoopers/InformationWeek Survey Verifies Link Between E-Commerce and Security

Risks: Global Information Security Survey Reflects IT Professionals' Views Worldwide", CMPNet, 31 August 1998. http://www.cmp.com/cmppr/releases/980831.htm, accessed 4 October 1999.

"Securing the E-Business 1999 Survey Results: Infosecurity Magazine Survey", Infosecurity Magazine, http://194.202.195.4/survey/results_1999.html, accessed 4 October 1999.

"Security Overview and Executive Summary", Infosecurity Magazine, July 1999. http://www.infosecuritymag.com/july99/chart1.htm, accessed 4 October 1999.

"The Status of Defense", http://www.sevenlocks.com/security/SCBStatusofDefense.htm, accessed 4 October 1999.

American Society for Industrial Security/PricewaterhouseCoopers, "Trends in Proprietary Information Loss Survey Report", http://www.pwcglobal/External/docid/36951F0F6E3C1F9E85267FD006348C5, accessed 27 October 1999.

Ascierto, Jerry. "High-Tech Theft Abounds: Study Suggests a $5 Billion Impact in Hardware Theft," Electronic News [1991], v45 i12 [March 1999]: 10 – 11.

Belcher, Tim and Elad Yoran. "Riptech Internet Security Threat Report: Attack Trends for Q3 and Q4 2001", Riptech Inc, January 2002. http://www.riptech.com/pdfs/Security%20Threat%20Report.pdf; accessed 6 February 2002.

Cole, Richard B. "What Trends Are Shaping Security's Future?" Security Management, v42 n7 [July 1998]: 150 – 152.

Computer Security Institute, "1999 CSI-FBI Survey Results", http://www.gocsi.com/summary.htm, accessed 44 October 1999.

Computer Security Institute, "Annual Costs of Computer Crime Rise Alarmingly: Organizations Report $136 Million in Losses", 4 March 1998. http://www.gocsi.com/preleall.htm, accessed 4 October 1999.

Computer Security Institute, "Cyber Attacks Rise From Outside and Inside Corporations: Dramatic Increase in Reports to Law Enforcement", 5 March 1999. http://www.gocsi.com/prelea90301.htm, accessed 7 July 1999.

Computer Security Institute, "The Cost of Computer Crime", http://www.gocsi.com/losses.htm, accessed 4 October 1999.

Computer Security Update, "Business Not Prepared for E-Risks," Computer Security Update, May 1, 2003, Boynton Beach. Accessed via Proquest May 31, 2003. http://proquest.umi.com/pqdweb?Did=000000325723601&Fmt=3&Deli=1&Mtd=1&Idx=1&Sid=5&RQT=309

Dalton, Gregory. "Acceptable Risks" InformationWeek Online, 31 August 1998. http://www.informationweek.com/698/98iursk.htm, accessed 4 October 1999.

Ernst & Young LLP. "2nd Annual Global Information Security Survey", Ernst & Young LLP, 1998. http://www.ey.com/security, accessed 4 October 1999.

Fisher, Dennis, "Cyber-Attack Costs Down, Says Survey," eWeek Electronic Magazine, http://www.eweek.com/article2/0,3959,1112163,00.asp (29 May 2003).

Germain, Colin, "Actual and Perceived Security Risk", 15 September 1997, http://www.soft.net.uk/cgermain/security.html, accessed 7 July 1999.

Howard, John Douglas. An Analysis of Security Incident on the Internet 1989 – 1995. PhD Dissertation, Carnegie Mellon University, 1997.

Huff, Darrell and Irving Geiss. "How to Lie with Statistics." WW Norton & Co, New York: 1954.

Kerstetter, Jim and John Madden. "Web Attacks Raise Chilling Questions for IT," Zdnet eWeek, 11 February 2000. http://www.zdnet.com/eweek/stories/general/0,11011,2436607,00.html, accessed 3 August 2000.

KPMG. "National Computer Security Survey 1996", http://kpmg.co.uk/uk/services/irm/survey/, accessed 4 October 1999.

NCC Info, "Information Security Breaches Are A Major Threat to British Business, According to NCC's Latest Survey", 24 March 1998. http://www.ncc.co.uk/nccinfo/21.html, accessed 4 October 1999.

NCC Info, "NCC Puts Business Continuity First at the Infosecurity 98 Exhibition", 28 April 1998. http://www.ncc.co.uk/nccinfo/infosec.html, accessed 4 October 1999.

NetSafe, "Information Theft in the Computer Age. Surveying the Scene: Information Theft 1995 to 1997" http://www.ozemail.com.au/~netsafe/95-97.html, accessed 16 November 1999.

Panettieri, Joseph C. "Information Security Survey", InformationWeek, 27 November 1995. http://www.hermesgroup.com/whitepapers/security/survey.html, accessed 4 October 1999.

Piscitello, David and Stephen Kent, "The Sad And Increasingly Deplorable State Of Internet Security," Business Communications Review; Hinsdale; Feb 2003. Accessed via Proquest May 31, 2003. http://proquest.umi.com/pqdweb?Did=000000290298601&Fmt=4&Deli=1&Mtd=1&Idx=17&Sid=6&RQT=309

Riptech, "Riptech Releases Groundbreaking Internet Security Threat Report", 28 January 2002. http://www.riptech.com/newsevents/release020127.html; accessed 30 January 2002.

Sustaita, David, "Security Awareness Training Quiz - Finding the WEAKEST link!" August 13, 2001; http://www.sans.org/rr/papers/47/396.pdf, accessed May 31, 2003.

Tan, Ding, "Quantitative Risk Analysis Step-By-Step"' December 2002, http://www.sans.org/rr/papers/5/849.pdf, accessed May 31, 2003.

U.S. General Accounting Office, "GAO Report to the Committee on Government Affairs, U.S. Senate: Information Security Serious Weaknesses Place Critical Federal Operations and Assets at Risk", September 1998, http://www.gao.gov/archive/1998/ai98092.pdf, accessed May 31, 2003.

U.S. General Accounting Office, "GAO Report to the Chairman, Special Committee on the Year 2000 Technology Problem, U.S. Senate: Critical Infrastructure Protection Comprehensive Strategy Can Draw on Year 2000 Experiences", October 1999, http://www.gao.gov/archive/2000/ai00001.pdf; accessed May 31, 2003.

U.S. General Accounting Office, "GAO Report to the Chairman, Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives: Information Security Serious and Widespread Weaknesses Persist at Federal Agencies", September 2000, http://www.gao.gov/new.items/ai00295.pdf, accessed May 31, 2003.

U.S. General Accounting Office and The National State Auditors Association, "Management Planning Guide for Information Systems Security Auditing" December 10, 2001, http://www.gao.gov/special. pubs/mgmtpln.pdf, accessed May 31, 2003.

WarRoom Research LLP. "Summary of Results for Information Systems Security Survey", 21 November 1996, http://warroomresearch.com/ResearchCollabor/SurveyResults.htm, accessed 4 October 1999.

Yazar, Zeki, "A Qualitative Risk Analysis And Management Tool – CRAMM", 2002, http://www.sans.org/rr/papers/5/83.pdf, accessed May 31, 2003.

About the Authors

Julie J.C.H. Ryan received her D.Sc. from The George Washington University (GWU) in Engineering Management and Systems Engineering. She holds an M.L.S. in Interdisciplinary Studies from Eastern Michigan University and a B.S. from the United States Air Force Academy. She is currently an Assistant Professor at GWU. Her research interests include information security, knowledge management, international relations, and information warfare. She worked for 18 years as an information security specialist, systems engineer, intelligence data analyst, and policy consultant prior to her academic career. She is the co-author of "Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves" (2000, McGraw-Hill).

Theresa I. Jefferson received her D.Sc. from The George Washington University (GWU) in Engineering Management and Systems Engineering. She holds an M.S. and B.S. in Operations Research from GWU as well. She is currently an Assistant Professor at GWU, where she is the Lead Professor for the Software Engineering and Information Systems Management concentration in the Engineering Management and Systems Engineering Department. Her research interests include information systems management, electronic commerce, human computer interface design issues, and computer system ergonomics.