1-2008

From Hindsight to Foresight: Applying Futures Research Techniques in Information Systems

Paul Gray

Claremont Graduate University and University of California, Irvine, paul.gray@cgu.edu

Anat Hovav

Korea University Business School

Follow this and additional works at: https://aisel.aisnet.org/cais

Communications of the Association for Information Systems

CAIS

FROM HINDSIGHT TO FORESIGHT: APPLYING FUTURES RESEARCH TECHNIQUES IN INFORMATION SYSTEMS

Paul Gray

Claremont Graduate University and University of California, Irvine

paul.gray@cgu.edu

Anat Hovav

Korea University Business School

Abstract:

Although much IS research deals with evaluating and improving existing information systems, researchers are also called upon to think about the future, particularly beyond organizational boundaries. Examples include: the potential impact of socio-technical phenomena such as the digital divide, digital rights management, security, and privacy. One way of forecasting the future is to extrapolate empirically observed relations (e.g. Moore's law). However, such extrapolations assume that the future is an immutable extension of the present and are usually limited to one or two dimensions. Externalities due to disruptive inventions, changes in regulations, tastes, competition, required skills, and more also need to be considered. This tutorial presents and explains three methodologies that take these possible changes into account to improve our understanding of the future: Delphi, cross impact analysis, and scenarios.

Keywords: cross-impact modeling, Delphi, modeling the future, scenarios

FROM HINDSIGHT TO FORESIGHT: APPLYING FUTURES RESEARCH TECHNIQUES IN INFORMATION SYSTEMS

I. INTRODUCTION

"There is no reason for any individual to have a computer in his home," Ken Olson, Founder and CEO of Digital Equipment Corporation, 1977

Although much IS research deals with evaluating and improving existing information systems, researchers are also called upon to think about the future of our field, of hardware, software, and specific applications and their implication on organizational strategy or society. One way of forecasting the future is to extrapolate empirically observed relations, such as Moore's law, or to use standard statistical forecasting techniques based on historical streams of data. However, extrapolation assumes that the future is an immutable extension of the present, leaving organizations vulnerable and unprepared to deal with sudden changes or ill-equipped to take advantage of unforeseen opportunities. Externalities, due to disruptive inventions, changes in regulations, tastes, competition, required skills, and more also need to be taken into account. The quotation above from Ken Olson is typical of the kind of off-the-top-of-the-head extrapolation[1] which harms an organization that does not do its homework in thinking about the future

Relatively few disciplines engage in futures research [Coats et al. 1994]. Yet, many organizations use techniques such as scenario planning as a strategic tool [Coats 2000]. Considering the impact of IT on business and social trends, it is valuable to engage in IT-driven futures research [Coats et al. 1994]. Using these techniques can also support the strategic value of information systems and their alignment with organizational strategy.

Assumptions of Futures Analysis

This tutorial is about three methods used for futures analysis. The methods share a common set of assumptions. First and foremost is that the future is not prewritten nor is it wholly determined by the past. However, present conditions and trends will continue along evolutionary lines UNLESS:

- Natural limits are approached.
- External changes occur.

External changes are inherently uncertain. Some aspects cannot yet be explained scientifically and some aspects (such as policy) depend on human choice. Attempts to guide the future through policy are based on the assessment of:

- Present and past conditions
- Possible future changes
- The extent to which future conditions can be altered by social resources

The desirability of social conditions is a value judgment. Desirability is not based on fixed criteria nor does it follow economic rationality.

The Planning Framework

In planning for the future, managers need to make estimates of what may occur either due to our own actions or those of others. Managers need to know what decisions are available to them and how these decisions interact with one another and with the environment. Of course, managers have preferences as to which outcomes they desire but have to deal with whatever outcome actually occurs. Not all outcomes are equally likely. Therefore, the probability of their occurrence needs to be estimated. For unfavorable outcomes, managers would like to be able to intervene and prevent them from happening or for ameliorating them. The planning problem is to decide: What should be done? When? How will we know the effects of our actions?

To move forward, we need to know where the uncertainties lie and how tractable they are. Tractability needs to be looked at not only in principle but in the cold, hard world.

---

[1] The quote by Olson was given at a meeting of the World Futures Society in 1977. Although widely disseminated, Olson claims the remark was taken out of context [Urban Legend Reference Pages: 2004].

Dealing with Uncertainty

The simplest way to deal with uncertainty is by fiat. That is the way it is done by CEOs in many firms. Unfortunately, fiat does not make the uncertainty go away. A second way, alluded to in the first paragraph, above, is to extrapolate historical data inside and outside the organization under the assumption that all developments are foreseeable. That, by itself, is a dangerous approach. The third approach is to elicit and evaluate judgments about the future from people who are "experts." The preferred method is to synthesize the results of approaches 2 and 3.

Experts

Experts, specialists, and authorities are people who are qualified to explore answers from a relevant disciplinary perspective. That includes practitioners and/or users. The range of possible experts is broad. For example, in a study of security, victims of identity theft, people who will need to live with the decisions made, and imaginative outsiders may qualify as experts from one or more perspectives.

When to Consult Expert Opinion?

Expert opinion may be a practical or a theoretical necessity. From a practical point of view, if an answer is absolutely needed and the available answers are not acceptable, expert opinion may be the only approach. From a theoretical point of view, opinion is required if the question is essentially judgmental.

Among issues for which expert opinion is an acceptable source of information are:

- Technological forecasts (particularly interdisciplinary changes)
- Social forecasts
- Desirability of a change
- Resolving the range of uncertainty
- Determining consumer needs
- Lack of documentation of current state
- Interpretation of history

The Role of Experts

Experts are sources of recall, critique, and speculation. Being experienced and knowledgeable in the field, they serve as memory, disclosing what has gone before and explaining why and how previous decisions were reached. They offer critiques of ideas, including interpreting the unintended consequences and evaluating the quality of new concepts. Chosen appropriately, experts imagine what can be done; estimate how well or poorly an idea will fare, and invent new ideas that expand the thinking beyond that of the group running the particular futures study.

When to Apply Futures Research Methods

The futures research methods discussed in this tutorial should be undertaken when:

1. The level of uncertainty about the future is high.
2. Limited historical data is available.
3. The number of entities (information technology and communications vendors, users, companies, government) is large.
4. The issue is important for current decision makers.
5. Major impact on information systems is involved and the issue is more than just technical.
6. The analysts involved know a considerable amount about the problem.

Organization of This Tutorial

This tutorial considers three futures research methods in sequence: Delphi (Section II), Cross-Impact Analysis (Section III), and Scenarios (Section IV). Conclusions are presented in Section V. We use excerpts from a sample case on organizational information security and privacy (presented in detail in appendix A) throughout this paper. Additional appendices describe technical details of the cross-impact analysis method used and the pitfalls of futures analysis. An annotated bibliography of the three methods follows the references.

II. THE DELPHI METHOD

The Delphi method [Linstone and Turoff 1977, 2002] uses the combined wisdom of crowds [Surowiecki 2004] to provide estimates as a function of time of the probabilities of events (occurrences such as an invention) and the evolution of trends (ongoing phenomena) when there is no source of factual data and a basis for opinion exists. The information sought is likely to affect decisions and policies.

SIDEBAR 1. THE ORIGINS OF DELPHI

The Delphi method was created in response to a problem posed by the Air Force to the RAND Corporation in the 1950s. The Air Force regularly assembled expert civilian groups in the Pentagon to obtain technical and/or policy advice about future directions. When they looked back at the transcripts of the sessions, they found that the advice they were receiving was typically that of one or two individuals who dominated the session, rather than the group as a whole. The dominant individuals would typically be the most respected or most vocal people present.[2] The Air Force concluded that the advice they received did not represent the views of all the panel members. Today, we call such output *groupthink*. It was RAND's task to develop a method for solving the problem.

The RAND research analysts decided the problem was that, since the panel met face to face, it was inevitable that the dominant voices would prevail. Therefore, the idea was that the panel of experts not be able to see one another or even know who favored which policy. That is how Delphi came to be.

The procedure involves a cyclical process. In each cycle, a set of questions is presented to a panel of subject experts in the topic of interest. Sample items might be:

- What is the earliest, most likely, and latest time when the market share of the LINUX operating system in businesses equals that of Windows?

- What is the probability that PCs with Windows operating systems will be secure against attacks by Trojans, worms, and other malware in 2010? In 2015? In 2025?

- Given the trend of PC sales in Africa since 2000, how many PCs do you forecast will be sold in Africa in 2010, 2015, 2025?[3] (Input provided to panelists includes sales 2000-2006)

Anonymity is provided to each respondent so that, when they make their estimates, they are not influenced by the responses of other members of the panel. Anonymity prevents groupthink [Janis 1989], or biased judgment under uncertainty [Tversky and Kahneman 1993]. The panelists are typically dispersed in space and time.

A Delphi survey is administered in rounds and usually run by a facilitator.[4] The responses from each round are tabulated and fed back to the group. Typically, people who provided extreme estimates (the smallest and largest values) are asked to state their reasons, and their opinions are circulated to the panel for each round after the first. The rounds stop when either consensus or dissensus occurs. A consensus can be measured by using traditional statistical tools such as cluster analysis or distance from the mean. The desired beta[5] should be determined before the session begins. Experimental results indicate that good forecasts can be obtained and that accuracy can be improved by asking people to state their degree of expertise for each item. If dissensus occurs on a particular question, it is an indication that expert opinion on the subject is divided.

A number of methods other than Delphi are available for obtaining expert opinions. These include:

• Literature surveys	• Individual insights (e.g., consultants)	• Polls
• Questionnaires	• Conferences and meetings	• Simulation and gaming
• Multidimensional Scaling		

When and How to Use Delphi

Delphi panels are suitable when:

- There is little or no source of factual data

- A basis for an opinion exists

- The Information is likely to affect decisions

---

[2] The method reduces "the influence of certain psychological factors, such as specious persuasion, the unwillingness to abandon publicly expressed opinions and the bandwagon effect of a majority opinion" [Gordon and Helmer, p. 5]

[3] Note that the time scale expands the further you go into the future.

[4] Although the facilitator who runs the Delphi knows the identity of the panelists and their responses, the panelists are not told who gave which response.

[5] Beta is the allowable Type II error. That is, the probability of Type II error the survey administrator is willing to accept.

A group is needed if the scope of the problem (e.g., PC security) is too broad for any one expert or the problem is so new that there are few experts. A group can be called for if there is a need to cross-fertilize ideas or to ensure that all aspects of the problem are covered.

Table 1 shows the relatively straight forward steps in a perfect Delphi. That does not mean that it is easy to implement. For a detailed discussion of Delphi, see the edited book by Linstone and Turoff [1972].[6]

Table 1. Steps in a Perfect Delphi[7]

1. Specify the subject and the objective.

2. Specify the forecasting mode to be used.

3. Specify all desired outcomes.

4. Specify the uses to which the results will be put, if achieved.

5. Design the study so that only judgmental questions[8] are included, the questions are phrased precisely, and cover the topics of interest.

6. Assemble a panel of respondents capable of answering all questions creatively, in depth, and on schedule.

7. Provide respondents with all relevant historical data.

8. Make sure that the facilitator collates the group responses consistently and promptly.

9. Make sure that the respondents are explicit about the grounds for their estimates, interpretations, and recommendations.

10. Analyze the data.

11. Probe the methodology and the results to identify any important needed improvements.

12. Create a paper or report and present the result to a journal or to management.

Creating the Delphi Questionnaire

Delphi questions can be put in a number of forms, depending on the nature of the inquiry being made. A particular Delphi questionnaire will contain a mix of question types. Table 2 shows some examples together with example responses. Be aware that devising a good Delphi questionnaire, like creating any social science questionnaire, is not done lightly. Run a pilot test on a small group (e.g., doctoral or MBA students) and make sure that the language is clear, the terms are well-defined and that the questionnaire is internally consistent. Provide sufficient input information that respondents are able to make judgments.

Research Results on Delphi

A number of experiments were undertaken in the 1960s by one of Delphi's co-inventors, Norm Dalkey [1969]. He used UCLA graduate students and people at RAND as his subjects and asked them almanac-type questions, such as "the number of telephones in Uganda." Correct answers existed in almanacs and similar sources. The subjects were unlikely to know these answers but at least some of the subjects possessed some relevant knowledge. He used groups of 20 to 30 subjects, and asked them 20 questions in a typical session. In general, the subjects were able to make reasonable "estimates" for these, to them, uncertain questions. The basic results of these studies are shown in Sidebar 2.

The finding of Sidebar 2 and other reports can be summarized as:

•   The spread of opinion narrows after the second round and the median, more often than not, shifts toward the true answer.

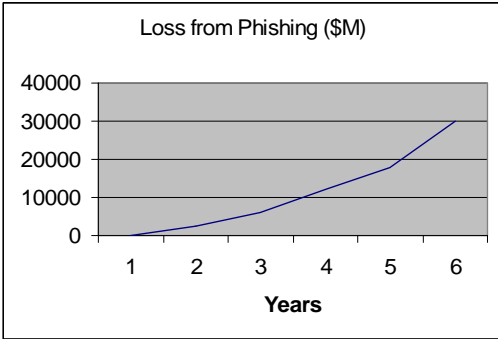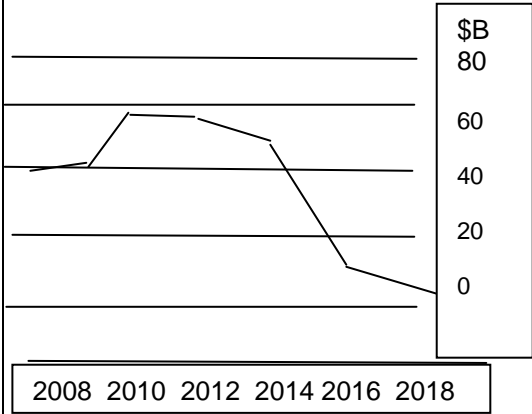•   Delphi interactions generally produce more accurate estimates than face-to-face meetings.

---

[6] The Linstone-Turoff book was reprinted in 2002 and is available on the Internet at http://is.njit.edu/pubs/delphibook/.
[7] This table is based on material developed by the late Olaf Helmer when he was at the University of Southern California in the 1970s.
[8] Nonjudgmental questions should be included only in extreme cases

- In general, the narrower the range of opinion, the more accurate the answer.
- Self-appraised expertise is a powerful indicator of accuracy.
- In the experiments, accuracy of the respondents improved when they were allowed 30 seconds for deliberation. Shorter or longer intervals (up to four minutes) led to increased error.

Table 2. Example Delphi Questions

Type	Subject	Example	Hypothetical response
Candidate events	Technological development	A virus is created that cannot be contained or countered	2008 2010 2012 2014 2016 2018 Never E M L
Trend	Total U.S. dollar loss from phishing attacks	Loss from phishing 2001-2006 is shown. Please estimate the trend values for the years 2008-2018	 2008 2010 2012 2014 2016 2018
Category	Social acceptance of security measures	Prob. of occurrence by given time • Cameras at traffic lights • Fingerprint identification of all PC users • Cell phone locators • Monitoring of TV channels selected	(see table below)
List of possibilities	M-commerce developments	Open ended question: List m-commerce developments. If possible, give their probability of occurrence versus time	Advertisement for nearest restaurant P=.3 by 2010

For the Category row, the hypothetical response table:

2008	2010	2012	2014	2016	2018
0.5	0.6	0.8	0.9	0.95	1.0
E		M		L	
M	L				
0.01		0.2			0.4

Note: E,M,L are Earliest, Most Likely and Latest time of occurrence

---

SIDEBAR 2: RESULTS OF DELPHI STUDIES

Size of group. The average error of the group responses declined monotonically with the size of the group, with diminishing returns with increasing size. Roughly, one half of the individual error was observed with groups of seven members. An additional 20 members reduced the average group error by an additional 10 percent. The reduction of error with size of group is analogous to, but not identical with, the rule for the dispersion of the sample mean in random sampling.

Iteration with feedback. There was monotonic reduction in the dispersion of individual responses (convergence) with iteration, again with diminishing effect with additional iterations. However, the accuracy of the group answer improved with the first iteration and fluctuated with additional iterations.

Dispersion. Smaller dispersion was associated with a greater likelihood of the group being correct. The average group error was approximately two-thirds of the observed dispersion.

Individual and group self-ratings. In may of the exercises, individuals were asked to rate their confidence in their answer to each question on a scale of 1-5 where 5 meant "I know the answer" and 1 meant "I'm just guessing." A group self-rating could then be computed for each question by taking the average of the individual ratings. Between a group self-rating of 1.2 and 4, average error dropped by a factor of 5.

Group self-rating and sample dispersions are thus valid, if rough, indicators of accuracy. Combined, they are even stronger. For cases of self-ratings of 2 or better and dispersion of .5 or less and cases of self-ratings of 2 or less and dispersions of 1.5 or more there is a factor of 10 difference in accuracy. Since these results were for a specific type of subject matter, and a specific type of "expert, " the precise relationships cannot be transferred directly to other investigations, but they can be used as guides in evaluating the solidity of elicited judgments. Low self ratings and large dispersions probably indicate unreliable results.
Source: Dalkey [1969]

Variations on Delphi

Variations on the standard Delphi process have been used or proposed. These variations include:

Round 0. Rather than the person or group organizing the Delphi selecting the questions and creating the questionnaire, a Round 0 is run in which the expert panel members are asked to define the subject matter often using open-ended questions. This approach typically expands and refines the range of topics covered. Thus, for example, in a Delphi on computer security, a panelist might introduce the possibility of a new physical form of identification or a different algorithm for encryption.

Self-rating. Rather than accepting all responses as equal, panelists are asked to rate their own degree of expertise on the question. These ratings can be used as weights when tabulating the responses. Dalkey's experimental results indicate that respondents tend to give better forecasts if they rate themselves high on expertise than if they don't. Such ratings are not perfect. For example, a small fraction rates themselves low on almost everything but their specialty whereas another small fraction claims expertise on everything.

Permanent Panel. For an organization running multiple Delphi sessions over time, recruiting panelists specifically for each inquiry becomes a major task. Helmer (personal communication) proposed setting up a large permanent panel (which he called D-net) from which people would be selected for a particular Delphi. Such a panel, for example, could include people who are retired, broadly knowledgeable, and computer literate.

Mini Delphi. Technologies such as Group Decision Support Systems (GDSS) [Gray 2008], can be used to assemble the panel so they can work simultaneously. For each round, the participants enter their values anonymously into the computer and give reasons for their values. For each question, two or more participants (typically those with extreme answers) are asked to discuss their points of view briefly. Panelists are then asked to revise their estimates anonymously. This approach is particularly useful as a way of gaining closure on the Delphi process after initial rounds.

Delphi Advantages

The Delphi process brings together a group of knowledgeable people to work on a problem and maintains their attention on the issues. By using a fixed set of questions that apply to the topic, it provides a framework in within which people can work. Because of anonymity, it minimizes the tendency to follow the leader, the tendency to accept specious persuasion, and other psychological barriers to communication. It provides an opportunity for all to be heard as individuals rather than on the basis of their labels (e.g., affiliation, field, reputation). Finally, it produces precise, documented records.

Delphi Disadvantages

Because of anonymity and separation from other panel members, people work without the stimulation of interaction with others enjoyed in face-to-face conferences.

When Delphi was first used, the entire process was paper and pencil. A round took a considerable amount of time because questionnaires and results of previous rounds had to be reproduced and mailed, followed by waiting for the responses to come in. The panel size would decrease with each round because some people would not respond within a reasonable time frame. All this changed with the introduction of e-mail and the Internet. Although rounds can be run more quickly, the problem of subjects' attrition is still there.

Conclusions on Delphi

The Delphi method is now well established. It is one way of incorporating expert opinion into forecasts, serves as input to cross-impact analysis (Section III), and provides insights useful for building scenarios. Although it is easy to discount expert opinion given the history of failure for many experts and the many pitfalls in running a Delphi, its use of the wisdom of crowds, where the crowd knows something about the subject, commends it for studies where other approaches fail.

The Delphi methodology is continually being improved. For example, at AMCIS 2007, White and Plotnick [2007] presented a paper on a dynamic voting scheme using Wikis that allows everything (voting, vote changes, new items, and discussion) to go on at the same time and be updated at any time by any participant. It permits hundreds and even thousands to deal with compiling an evaluated list by allowing people to focus on just those items about which they feel confident and concerned.

III. CROSS-IMPACT ANALYSIS

Cross-Impact Analysis

The Delphi method provides individual forecasts which are assumed to be independent of one another. In a sense, they are forecasts under the condition of all other things being equal. However, in the unfolding of events and trends, things are rarely equal. Since forecasts cover relatively long periods of time, the forecaster needs to recognize that the sequence in which events happen can (and does) change future events. For example, consider a forecast of the state of information privacy in the year 2020 based on today's technology and a Delphi study of three innovations: the introduction of a secure operating system, advances in preventives technologies, and a new uncontainable virus. The forecast will depend not only on the probability of the innovations as a function of time but also on the order in which they occur and on the impacts of the inventions on one another. The Cross-Impact method is an approach to modeling and evaluating these possible future changes and assessing their impacts on other events and trends. It goes back to work of the Futures Group of Glastonbury CT in the late 1960s. Seminal papers include Gordon and Hayworth [1968], Helmer [1972], and Enzer [1980].

The cross-impact model is the next step of sophistication beyond Delphi. It allows using the Delphi results in sensitivity analysis, scenario analysis, and policy planning. Cross impact is a stochastic, multi-period model run in simulation mode. Each run of the simulation creates a scenario by presenting snapshots that show when events occurred and what values trends will have

Cross-impact analysis recognizes that events are not independent of one another. Thus, for example, if hydrogen-powered cars are successful in a given time interval (t_j), the probability of vehicles that use competing energy sources becoming available in subsequent time periods (t_{j+1}, t_{j+2},…) may change. As another example, a Delphi panel might be asked to estimate, the probability as a function of time, when Linux market share will exceed that of Windows. If this estimate is used as the input to a cross-impact analysis of security, the cross-impact panel might be asked the implications of the Linux market share surpassing Windows: would the attacks on Linux increase (e.g., because hackers hack for economic or financial gain) or decrease (e.g., if most hackers are culturally motivated).

In cross-impact analysis, the Delphi respondents estimate the impact of the occurrence[9] of each event on the probability of occurrence of every other event. The probability estimates from the Delphi process and the cross-impact estimates are used in multi-period simulations that work as follows:

1. In each period, the simulation examines each event that has not yet occurred. It uses a random number generator to select the events that occurred in the period.[10]
2. The simulation then updates the probabilities of the events that did not occur based on the occurrence and non-occurrence of each of the other events. Note that the impact of a high probability event that does not occur affects other events in subsequent time periods more than events of low probability.

The output of the cross impact simulation presents the distribution of outcomes. The mechanics of cross-impact simulation are discussed in Appendices B and C.

Conclusions On Cross-Impact Analysis

Advantages of Cross-Impact Analysis

Traditional Delphi presents a single possible future from a forecast based on a set of current assumptions, potential events, and trends. Cross-impact analysis allows the analyst to account for the interdependencies among events and trends over time. Interdependence is particularly important when trying to analyze the future of socio-technical events. For example, the issue of information privacy is not only a matter of technological developments such as better countermeasures or more secure software, it is also imbedded in economic, ethical, and political issues, all of which interact with one another.

---

[9] As shown in Appendices B and C, the impact of non-occurrence can be determined from the impact of occurrence

[10] The choice is made in standard simulation style. A random number from 0 to 1 is drawn by the computer. If the random number is less than or equal to the probability of the event, the event is declared to have occurred; if the random number is larger than the probability of the event, the event does not occur.

Cross impact makes it possible to find and understand the multiple futures we face, and assess their probabilities so we can find policy options to deal with the multiple contingencies.

Limitations of Cross-Impact Analysis

Although the cross-impact concept is 40 years old, practical cross-impact analysis is still a work in progress. A number of methodologies have been proposed and some of these were implemented in specific studies. Each method solves some problems but not others. Unfortunately, we did not find any studies that compare the various approaches.

While the method uses mathematical computations extensively (see Appendices B and C), much of its input data comes from expert opinion such as from Delphi studies. The simulation models used in cross-impact analysis are simplified to make the computations tractable. The analyst is faced with tradeoffs of making the results accessible versus making them mirror the way things work in the real world.

Findings

In this section (and in Appendices B and C) we present a particular approach to cross-impact analysis. It is clear that cross impacts, such as those caused by disruptive technologies, exist. Simply using the Delphi forecasts often misses disruptive changes. Furthermore, Delphi results, by themselves, rarely take disruptions into account.

Cross impacts are also important when creating scenarios. Although each run of a cross-impact simulation is a scenario, it is rarely possible to use a single run as a complete scenario because its parameters don't always conform to the scenario space or because it violates one of the three basic principles of scenarios (see Section IV). However, when examining groups of similar outputs, they do provide insights, justification, and concepts for use in scenario building.

Additional approaches to cross-impact analysis are presented, for example in Linstone and Turoff [1972] and by the European Commission [2006]. Although cross-impact analysis is somewhat out of fashion at present, we believe it is a useful analytic tool that merits further development.

IV. SCENARIOS

Overview

Usually, business and government managers make decisions that shape the future of their organization[11] based on a particular vision of the future. Unfortunately, relying on a single vision is risky because the future involves great uncertainty and depends on a large number of variables whose values are unknown [Stout 1998]. Decision making under high levels of uncertainty tends to rely on groupthink [Janis 1989] or to be biased by current information [Tversky and Kahneman 1993]. A more realistic way to overcome these problems and understand the range of futures faced is to develop alternatives; that is, scenarios, which allow decision makers to create policies which cope with the unknowns [Stout 1998].

Scenarios are a way of communicating about the future. They are stories that describe how the world will be in terms that managers and other non-specialists can understand. That does not mean that they are arbitrary. As discussed in Gray and Hovav [2007], they are carefully worked out to reflect the logical implications of assumptions and forecasts about what the future will be like. Scenarios are an end product of a careful analysis, not the workings of the fertile imagination of a novelist or a science fiction writer. Scenario building is a discipline that involves many people from inside and outside the organization and typically describes future events and trends within a given set of assumptions and constraints.

Sidebar 3 shows a scenario that is in keeping with the running example described in Appendix A.

Sidebar 3. The "Big Brother" Scenario for 2020

The scenario is based on the assumption that the levels of technical security are high, yet the number of identity thefts resulting from hacking and social engineering continues to increase, leading to a "Big Brother" mentality.[12]

Technical security and software security. Companies invest large sums in the implementation of technical

---

[11] A few make decisions about the past. The classic (fictional) example is Winston Smith, the anti-hero of Orwell's dystopian novel *1984,* whose responsibility was to rewrite history whenever the present changed.
[12] See Figure 2 for additional scenario options for describing the future of identity theft.

countermeasures. Operating systems and other support software achieve 98 percent security. Best-practices and standards provide companies with guidelines for secure architecture.

Technical countermeasures versus "soft" measures. Most security efforts are channeled toward technical countermeasures. There is little emphasis on training and educating users. The technical superiority of the security efforts is assumed to take care of identity theft threats. Organizations ignore the need to develop a "security culture."

Social engineering. Hackers find new ways to hack into systems. Most of them rely on social-engineering methods (such as phishing) and on poor access control procedures in organizations.

International privacy regulations. The U.S, like most developed countries, signs a treaty for worldwide standards for privacy. The penalties for privacy breaches and identity thefts in these countries increase. However, a number of fourth-world countries do not sign this treaty and are used as breeding grounds and safe havens for hackers.

The Internet. To increase Internet security, the U.S. government imposes constant monitoring of data. To avoid penalties, Internet service providers and telecommunications companies monitor all traffic that passes through their systems and report any unusual activity to law enforcement agencies.

Use of biometrics and other invasive security technology. To combat the increase in identity thefts, companies and government agencies employ biometric technologies. Digital cameras that feed into national face recognition systems are implemented at every street corner.

Negative public response. The public is outraged by the gross invasion of privacy that does not stop the continuing increase in identity theft. The issue becomes an ongoing part of the political arguments in the election cycles for the executive branch and for Congress.

Why Do Organizations Use Scenarios?

To survive, organizations adjust to their changing environments. Adjusting is particularly critical when an industry experiences radical changes or discontinuities that change the basis of competition [Tushman and Anderson 1986]. Organizations achieve alignment with their environment by using one or more of the following strategies:

1. *Creating the future* by changing the basic assumptions (or the rules of the game) as was done by Microsoft, Intel, and to some extent Cisco [Gawer and Cusumano 2002]. Applegate et al. [1996] point out that organizations that create the future need enough resources to sustain the direction they started or they will be overtaken by second or later movers.

2. *Reacting to environmental changes after the fact.* This strategy is the most common and is often taken by middle adopters. This approach is risky if the change creates a hostile environment and may result in the demise of organizations and even complete industries. For example, many of the top hi-tech companies of the 1980s no longer exist.

3. *Forecasting potential environmental changes.* This strategy, often adopted by leaders, involves forecasting possible environmental changes and either planning for them or adopting policies that can alter the course of events.

Scenarios can help managers achieve the third strategy since scenarios examine the issues to be resolved, the time relations, interactions, and the logical consequences. Scenarios are most powerful when several are used together to present alternative views of the future as seen from the present. They enable humans and organizations to take actions that influence the future. That is, scenarios are a policy analysis tool [Boroush and Thomas 1992]. For example, if a scenario indicates that undesirable future has high probability of occurrence, the organization can take actions to make it much less likely to happen, such as lobbying, merging, changing its business practices, or innovating.

A-Priori Assumptions about Scenarios

One of the greatest dangers of poor scenario building is information overload—scenario builders often include a large number of variables regardless of their relevance to the subject or the issue at hand [Morrison 1994]. To develop high quality scenarios, a set of assumptions and constraints should be established in advance [Stout 1998]. For example, in creating alternative scenarios about hacking activities over the next 5-10 years, the characteristics shown in Table 3 need to be defined.

Table 3. Considerations in Scenarios about the Future of Hacking	
Factor	**Consideration**
Purpose	What is the study trying to determine? What decisions need to be made based on the scenarios?
Domain	What domain is being studied?
Geopolitics and economics[13]	Do levels of hacking differ between U.S. and non-U.S firms? What are the economic impacts?
Time frame	A time frame must be defined. For example, the scenario for a one year future will, most likely, be different than for a 10-year horizon.
Unit of Analysis	Scenarios differ depending on whether the focus is the individual, organizations, and/or society.
Organizational Characteristics	Scenarios typically apply to a specific organization or government. e.g., Large organizations may be targeted by hackers for political or publicity gain.

Scenario Development Principles

Four principles in creating scenarios are [Boroush and Thomas 1992; Morrison 1994]:

1. Identify the critical (or possible) choices that the subject (individual, organization, society) is likely to face The list of choices may be developed by using Delphi and/or qualitative discussions.
2. Identify (through Delphi or other means) the key drivers that might shape the future of the subject or issue.
3. Model or create the scenario space (see below). Select the values to be associated with each variable defined for the scenario space, using qualitative discussions, Delphi, and cross-impact analysis. Make sure that the values chosen lead to a range of outcomes that cover the scenario space.
4. Analyze the implications. Once the scenarios are created, they can (and should) be used to determine strength and weaknesses of the organization and to create alternative contingency policies and strategic plans that enable the organization to cope with the different scenarios. That is, the scenarios developed need to be followed by organizational actions [Stout 1998].

To use scenarios as input to organizational long-term strategic planning, steps 2, 3, and 4 should be repeated. A cyclical approach helps to identify the impact of selected actions (policies, new product development, lobbying). For example, if a scenario calls for establishing international standards for information security, that variable becomes fixed and a new scenario space is created (step 2), leading to a new set of scenarios (step 3) and a potential new set of internal policies and management decisions (step 4). If the result is favorable, the organization should consider supporting the development of international standards either financially or via lobbying. If the result is unfavorable (e.g., the organization is likely to lose market share), the organization could object to the proposed standards or develop alternative products.

Characteristics of Scenarios

Scenarios must adhere to three principles. They must be:
1. Possible
2. Plausible
3. Internally consistent

Possible implies that there are no barriers to the events described occurring. Thus, for example, a scenario can not assume speeds faster than light.

Plausible implies that the reader of the scenario would believe that the events could occur. For example, physically isolating all computers in a firm from the Internet to ensure information privacy is a possible but not a plausible scenario.

Internal consistency, as its name implies, requires that all parts of the scenario are consistent with one another. For example, a scenario in which organizations rely on law enforcement to protect them against hackers and at the same time posit that company personnel do not report hacking attempts is inconsistent.

---

[13] Source: Coates et. al. [1997]

The Scenario Space

Scenarios are embedded in a scenario space. The space is defined by variables whose values are specified. For example, in studying computer security, we might choose

- Identity theft and privacy breaches as one dimension, and
- Software security as the other

For this simple, two-dimensional space we might create four scenarios, one for each combination. Figure 1 shows the scenario space. Sidebar 3 at the beginning of this section is a brief scenario based on the High Technical Security Level, High Identity Theft Level in Figure 1.

High Technical Security Level	Trusted	Big Brother
Low Technical Security Level	Status Quo	Chaos
	Low Identity Theft Level	High Identity Theft Level

Figure 1. Sample Scenario Space

Here the four scenarios in the scenario space would describe:

1. High software security level, low identity theft; a highly trusted environment

2. High software security level, high identity theft; a "Big Brother" environment where every transaction is monitored, tracked and audited to ensure the integrity of the data yet social engineering attacks escalate identity theft

3. Low software security level, low identity theft; the status quo

4. Low security level and high identity theft; chaos from neglect of improving security, resulting in extreme government security regulations and law enforcement crackdown to reduce identity theft.

A more complex scenario space for the future of organizational Information security might use six dimensions: (1) regulatory activities and compliance; (2) technological advances and preventive tools; (3) hacker activity and culture; (4) human engineering; (5) cost; and (6) risks and legal liability. If we assume that each variable can take on only two values (high and low), then we have 64 (i.e., 2^6) combinations, each of which defines a scenario. Of course, in creating a set of scenarios it is not necessary or possible to present all 64 combinations. Note that some combinations are implausible or impossible and can be excluded. Only scenarios for combinations deemed significant would be created.

The Practicalities of Scenario Development

The practical steps in developing a scenario are:

Select system variables of interest	Define the variables of interest (a manageable number of key variables, potential future events, and relations to the socio-technical and economic variables).
Forecast system parameters	Use Delphi, trend and cross-impact analysis to set the values of the system parameters to be used in the scenario.
Select scenario space	As indicated in the previous subsection, the space is determined by the variables that are expected to be the scenario drivers.
Perform a consistency check	Use forecasts in scenario space, simulation models, historical relations to perform a consistency check.
Develop measurements	Develop surrogate measurements to help the organization determine if it is heading towards one scenario or another.
Write the scenarios	See the next subsection.
Analyze and develop policies	Develop policy options and determine mismatches between current policy and future needs.

Writing Scenarios

Scenarios for a given time horizon can be written from three points of view:

1. A newspaper story written on some date in the future (e.g., August 11, 2020) describing the situation on that day. No history or motivation is given. Such a scenario would assume that everyone knows what happened previously. This type of scenario describes a known phenomenon in terms that are easy to understand [Coats 2000].

2. A history written on, say, August 11, 2020 that describes the series of events that occurred between now and then and led to the future situation.

3. A forecast that starts in the present and shows the evolutionary path which results from the assumptions in the scenario space. This approach leads the reader forward into the future rather than approach 2, which works backwards from the end-point. The evolutionary approach is the one most often used for strategic planning and is the one we favor.

In writing a scenario, it is important to discuss:

- The stakeholders involved and, if possible, the effect of the scenario on these stakeholders
- The values given to parameters in the scenario. The values need to be consistent with the assumptions of the scenario being written.

For example, scenarios for coping with security issues by making software a completely outsourced service result in a different role, size, and technical composition of the IS department than a scenario that is based on technological advances and preventive tools.

Because each scenario takes considerable time to create, only a few can be generated. Researchers and managers are advised to select a small number of scenarios (e.g., four or six) from a scenario space which together represent diverse future outcomes. In general, it is considered appropriate to present an even number of scenarios (e.g., four); an odd number leads managers to select the middle scenario as most likely and avoid consideration of the others [Morrison 1994]. Furthermore, two scenarios are too few because managers can easily select only the more favorable one, defeating the purpose of scenarios.

Avoiding Scenario Pitfalls

In writing scenarios, it is important to avoid three pitfalls:

1. Confusing the scenario and the outcome
2. Confusing the scenario and the forecast
3. Assuming that scenarios are static

Scenarios Are Not the Outcome

The users of the scenario should not assume that any scenario generated precisely defines the future or that it is pre-ordained and nothing can be done about it. This assumption, for example, leads to ignoring policies (or decisions) that can influence the future of the firm, thus defeating the purpose of using scenarios.

Scenarios Are Not a Forecast

Similarly, the user should not assume that a particular scenario is the forecast of the future when it is only one of several potential alternative futures. Although there is a nominal forecast that represents the most likely outcome, managers should not ignore other scenarios. Sidebar 4 shows an example of the errors that resulted when extrapolating present trends created a single forecast.

Scenarios Are Not Static

Assumptions and conditions change rapidly (especially in volatile areas such as information systems and technology). Thus, a set of scenarios cannot be used as is over extended time periods.[14] Scenarios must be reconsidered and reevaluated as conditions change. Making decisions or setting policies based on outdated scenarios can create more harm to an organization than not using scenarios at all.

---

[14] For example Shell, a company known to use scenarios as part of their long-term strategic planning, reevaluate their scenarios annually [Coats 2000].

Sidebar 4. Example of Error from Relying on Extrapolation as THE Scenario

In the 1970s and early 1980s, robustness of computer systems was thought to be a major driver in their future development and adoption. Mathematical modeling of systems (such as the relational databases, the MULTICS O/S, and the ADA programming language) were used to prove correctness. Organizations were willing to pay for robust systems. A scenario describing departure from that trend was hard to imagine and was assigned a low probability of occurrence. It was unimaginable then that the modus operandi would shift radically in the 1990s, where low cost, ease-of-use, and speed to market, would replace robustness and completeness. Yet, that is precisely what happened with the introduction of personal computers, Intel architecture, and the Windows Operating systems [Gawer and Cusumano 2002; Anderson 2001]. High-tech companies, such as Digital Equipment Corporation (DEC) that did not include this seemingly low probability scenario in their deliberations were unable to plan for the shift or adjust to it. They no longer exist.

Conclusions on Scenarios

As discussed at the beginning of this section, scenarios are stories about alternative futures. They provide a way of communicating with managers and non-experts. Using scenarios helps in understanding the implications of different outcomes and in making decisions as to which outcome to encourage.

Scenario building is both art and science. Although it involves experts that follow the processes described in this section, it is rare that two scenario builders will create the same scenarios for a given problem. A key success factor of scenario building is the ability to duplicate the process [Coats 2000].

The values of the scenario drivers and the requirement that scenarios must be internally consistent create a tendency to develop pure scenarios, that is, scenarios in which everything is positive or everything is negative, or everything is average. Of course, the real world is not like this. A mix of outcomes will occur. Going too far in one direction tends to create scenarios that are ignored because they are not plausible. Unfortunately, there are no guidelines yet for creating mixed scenarios where some outcomes are guaranteed positive and some negative.

Scenarios are most valuable when:

1. The external environment is highly uncertain.
2. The environment might take plausible alternative trajectories.
3. A specific set of indicators can be developed to measure the driving forces and their likely impacts if they were to occur.

Scenarios are a basis for policy discussion. The objective is not to find the "most likely" scenario for the organization. Rather it is to understand the range of possibilities and develop plans and alternatives that can react to or influence whichever future occurs.

V. CONCLUSIONS

The three research methods described in this tutorial—Delphi, cross-impact, and scenarios—provide ways of analyzing and understanding the uncertain future that organizations face. They are particularly useful in dealing with large, messy problems where data is scarce and experiments cannot be performed. In many situations that involve dealing with the future, they are the only ways available for sense-making in a continually shifting world, in particular, in information systems, a field subject to continual change.

The concepts and the methodologies for performing Delphi and scenario studies, which go back over forty years, are well established. Cross-impact concepts are understood but the best way of performing such studies is still an open question.
 This tutorial stresses the positive aspects of the methodologies. As discussed in Appendix D, some pitfalls exist that need to be avoided. It is our judgment that, by applying these methodologies appropriately and making clear the limits of what can be done, Delphi, cross-impact, and scenarios are three ways to improve our understanding of the future.

REFERENCES

Anderson, R. (2001). "Why Information Security is Hard: An Economic Perspective, " *Proceedings of the Seventeenth Computer Security Applications Conference.* IEEE Computer Society Press. pp. 358-365.

Applegate, L., W. McFarlan, et al. (1996). *Corporate Information Systems Management: Text and Cases.* Chicago: Time Mirror Book.

Arditi, T. et al. (undated). "Cross Impact Matrix Method of Forecasting, " http://wwww.iit.edu/~iit/cross.html.

Boroush, M. A. and C. W. Thomas. (1992). "Scenarios for the Defense Industry After 1995, " *Planning Review* 20(3) pp. 24-29. May/Jun.

Bower, J. M. and C. M. Christensen. (1995). "Disruptive Technologies: Catching the Wave," *Harvard Business Review* 75(1) January-February.

Coats, J. (2000). "Scenario Planning," *Technological Forecasting & Social Change* 65, pp. 115-123.

Coats J., J. Mahaffie, et al. (1994). "Technological Forecasting: 1970±1993, " *Technological Forecasting and Social Change* 47, pp. 23-33.

Coats J., J. Mahaffie J., and A. Hines. (1997). *2025: Scenarios of US and Global Society Reshaped by Science and Technology.* Greensboro, NC: Oakhill Press, 1997.

Dalkey, N. and O. Helmer. (1963). "An Experimental Application of the Delphi Method to the Use of Experts," *Management Science,* Volume 9.

Dalkey, N. (1969). "Delphi: An Experimental Study of Group Opinion," The RAND Corporation Report 5888, 87 pp. http://www.rand.org/pubs/research_memoranda/2005/RM5888.pdf [consulted 8-16-07].

Enzer, S. (1980). "INTERAX—An Interactive Model for Studying Future Business Environments: Part I," *Technological Forecasting and Social Change* 12 pp. 141-159.

Enzer, S. (1980). "INTERAX—An Interactive Model for Studying Future Business Environments: Part II," *Technological Forecasting and Social Change* 17 pp. 211-241.

Enzer, S. and S. Alter. (1978). "Cross Impact analysis and Classical Probability: The Question of Consistency," *Futures* 10(6) pp. 227-239.

European Commission. (2006). "Cross-Impact Analysis, " http://forlearn.jrc.es/guide/2_design/meth_cross-impact-analysis.htm [consulted 7-7-07].

Futures Group. (1994). "Relevance Tree and Morphological Analysis," http://www.futurovenezuela.org/_curso/12-tree.pdf [consulted 7-9-07].

Gawer, A. and M. A. Cusumano. (2002). *Platform Leadership: How Intel, Microsoft and Cisco Drive Industry Innovation*, Boston, MA: Harvard Business School Press.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and R. Richardson. (2006). *2006 CSI/FBI Computer Crime and Security Survey*, San Francisco, CA: Computer Security Institute.

Gordon, T. and H. Hayward. (1968). "Initial Experiments with the Cross-Impact Matrix Method of Forecasting," *Futures* 1(2) pp. 100-116.

Gordon, T. and O. Helmer. (1964). "Report on a Long Range Forecasting Study," Report P-2982. The RAND Corporation http://www.rand.org/pubs/papers/2005/P2982.pdf.

Gray, P. (2008). "Nature of Group Decision Support Systems," in Burstein, F. and Holsapple, C. *Handbook of Decision Support Systems, Vol. 1*, Heidelberg: Springer Verlag.

Gray, P. and A. Hovav. (2007). "The IS Organization of the Future: Four Scenarios for 2020," *Information Systems Management* 24(2) pp. 113-120.

Günaydin, H. Murat. (undated). "The Delphi Method," http://www.iyte.edu.tr/~muratgunaydin/delphi.htm [consulted 7-7-07].

Helmer, O. (1972). "Cross Impact Gaming," *Futures* 4(2) pp. 149-167.

Ives, B., K. R. Walsh, and H. Schneider. (2004). "The Domino Effect of Password Reuse," *Communications of the ACM* 47(4) pp. 75-78.

Janis, I. (1989). " Groupthink: The Desperate Drive at Consensus at Any Cost, " in S. Otts, S, (ed.) *Classic Readings in Organizational Behavior.* Belmont, CA: Wadsworth Publishing Company. Volume 1, pp. 223- 232.

Linstone, H. A. and M. Turoff eds. (1977). *The Delphi Method: Techniques and Applications,* Belmont, MA:.Addison Wesley.

Linstone, H. A. and M. Turoff eds. (2002). *The Delphi Method: Techniques and Applications*, http://is.njit.edu/pubs/delphibook/

Communications of the Association for Information Systems

Linstone, H. A. (2002). "Eight Basic Pitfalls," Chapter VIII in Linstone, H. A. and M. Turoff eds. (2002) *The Delphi Method: Techniques and Applications.* http://is.njit.edu/pubs/delphibook/.

Morrison, J. (1994). " The Future Tool Kit, " *Across the Board* 3(1) pp. 18-25.

Sackman, H. (1975). *Delphi Assessment: Expert Opinion, Forecasting, and Group Process.* Lexington, MA: Lexington Books.

Schoemaker, P. (1995). " Scenario Planning: A Tool for Strategic Thinking, " *Sloan Management Review* 36 (Winter) pp. 25-40.

Simon, S. " Definition: Likelihood Ratio, " http://www.childrens-mercy.org/stats/ definitions/ likelihood.htm Last consulted 7-14-07.

Stout, D. (1998). " Use and Abuse of Scenarios, " *Business Strategy Review* 9(2) pp.27-36.

Surowiecki, J. (2004). *The Wisdom of Crowds,* New York: Anchor Books.

Tversky, A. and D. Kahneman. (1993). " Judgment under Uncertainty, " In D. Kahneman, P. Slovic and A. Tversky (eds.) *Judgment under Uncertainty: Heuristics and Biases*, New York: Cambridge University Press pp. 3-20.

Tushman, M. L. and P. Anderson. (1986). "Technological Discontinuities and Organizational Environment," *Administrative Science Quarterly* 31(3) pp. 439-465.

Urban Legend Reference Pages. (2004). http://www.snopes.com/quotes/kenolsen.asp.

White, C. and L. Plotnick. (2007). "A Dynamic Voting Wiki Model," *AMCIS 2007*, Keystone, CO.

ANNOTATED BIBLIOGRAPHY

Arditi, T. et al. (undated) Cross Impact Matrix Method of Forecasting http://wwww.iit.edu/~iit/cross.html.

 [[A short but excellent summary of cross impact. Useful for getting started. Many of its ideas appear in Section III of this paper. The paper was one in a series developed by the Illinois Institute of Technology Department of Civil and Architectural Engineering as part of a study of Forecasting the Impact of Information Technologies in the *Project Management Book of Knowledge*. Unfortunately, the version retrieved from the Internet is undated. No author is given but the project was under the direction of T. Arditi.]]

Dalkey, N. and O. Helmer. (1963). "An Experimental Application of the Delphi Method to the Use of Experts," *Management Science,* Volume 9.

[[The original journal publication on the Delphi method by its inventors.]]

Gordon, T. and O. Helmer. (1964). "Report on a Long Range Forecasting Study," Report P-2982. The RAND Corporation http://www.rand.org/pubs/papers/2005/P2982.pdf.
[[A 72-page report on RAND's initial work on Delphi. The authors cite the paper by Dalkey and Helmer as the original publication on the subject.]]

European Commission. (2006). Cross-Impact Analysis http://forlearn.jrc.es/guide/2_design/meth_cross-impact-analysis.htm.

[[One in a series of papers on futures research by the Joint Research center of the European Commission, a part of the European Union (EU)]]

Gray, P. and A. Hovav. (2007). "The IS Organization of the Future: Four Scenarios for 2020," *Information Systems Management* 24(2) pp. 113-120.

[[An example of scenarios. Shows four scenarios based on differing assumptions about the reliability of international telecommunications and the value placed on computerization by business and society]]

Linstone, H. and M. Turoff. (2002). *The Delphi Method, Techniques and Applications* http://is.njit.edu/pubs/delphibook/.

[[A publicly available, copyrighted version of the book by Linstone and Turoff published in 1975. It is a comprehensive summary and includes contributions by many of the initial workers on Delphi. Given its 1975 time of appearance, it is restricted to paper-based Delphi. Fundamental reading to get into Delphi.]]

Schoemaker, P. J. (1995). "Scenario Planning: a Tool for Strategic Thinking," *Sloan Management Review* 36(2) Winter, pp. 3-33.

[[This *Sloan Management Review* is perhaps the most widely read and cited article on using scenarios for planning.]]

Turoff, M. and S. R. Hiltz. (1996). "Computer Based Delphi Processes," http://web.njit.edu/~turoff/Papers/delphi3.html.

[[This material is a chapter in a book by Adler, M. and Ziglio, E. (editors), *Gazing Into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health*, London, Kingsley Publishers (1996). This chapter discuses how the computer-based Delphi differs from the paper-based version. It stresses the relations to computer supported cooperative work, GDSS, and distributed computing.]]

APPENDIX A. THE RUNNING SCENARIO ON COMPUTER SECURITY

The Issue at Hand

From the point of view of the public and of many executives, the present levels of privacy breaches and identity theft are unsatisfactory and must be dealt with. The issue is which actions to take to improve the situation. In addition to finding technical countermeasures, social countermeasures can be applied, including changes in economics, regulations, and the trust environment.

The purpose of the computer security scenario is to examine the implications of proposed changes on individuals, organizations, and society.   To help the reader understand what goes into building scenarios, we present:

- An example of a major identity theft
- Descriptions of technologies, countermeasures, and secure software
- Sample Delphi questions that would be used in creating alternative scenarios

Background

An Example of Identity Theft and Breach of Privacy.

A major security breach was discovered on December 18, 2006. TJX, the holding company for retailers such as TJMaxx and Marshalls, discovered that hackers penetrated its computer systems.[15] Over 96 million customer data records were stolen, making it the largest privacy breach in the history of U.S. commerce. TJX notified the authorities, and an investigation into the matter ensued. It was not until a month later that TJX alerted its customers and the public. As of August, 2007, details about the exact nature of the attack are scarce and the identity/origin of the attackers is unclear.

The TJX attack resulted in both a breach of privacy and potential identity theft. Among the consequences were:

1. Wal-Mart (a firm completely unrelated to TJX) lost $8 million in merchandise bought with bogus gift cards that used TJX stolen credit information. (http://www.computerworld.com/blogs/node/5670)
2. Hundreds of banks had to re-issue credit cards to affected customers. (Mass. credit union billed TJX for $590,000, the bank's estimated cost to reissue credit cards.) (http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9023778)
3. A number of other class-action lawsuits by individuals who were affected by the case and by a number of banks and bank associations[16] are pending.

Thus far, the financial damage to TJX is minimal:

1. In the first quarter of 2007, TJX recorded a charge of approximately $5 million, or $.01 per share, for costs incurred, which include costs to investigate and contain the intrusion, enhance computer security and systems, and communicate with customers, in addition to technical, legal, and other fees.

---

[15] The data on TJX are based on the situation on August 15, 2007 when this section was last updated. Additional developments after that date are not included.
[16] For example see https://www.massbankers.org/pdfs/DataBreachSuitNR5.pdf for the class action lawsuit by the Massachusetts Bankers Association and the Maine Association of Community Banks and Individual Banks, and see http://www.boston.com/business/globe/articles/2007/01/30/ for an example of a lawsuit by an individual customer.

2. By the third quarter, TJX reported a $0.25 cost per share.
3. Yet, the impact on TJX overall share price was minimal (Reported sales actually increased). The TJX stock tracked the ups and downs of the market.
4. As of August, 2007, no publicly reported legal penalties were imposed by the Federal Trade Commission.

Protective and Preventive Security Technology

People and organizations use firewalls, intrusion detection systems (IDS), antivirus and anti-spam software, and access control mechanisms to secure data on their computers. Overall, the Computer Security Institute (CSI) reports that in 2006, organizations spend from $128 to $1,349 per employee[17] on information security. Yet, most organizations studied by CSI during the same time period reported at least one external security attack [Gordon et al. 2006]. Hackers are well organized and are able to find vulnerabilities in most current systems. IDS can be circumvented, encryptions can be cracked, user identification and passwords can be broken using brute force attacks (such as dictionary attacks) or via social engineering.

Potential Countermeasures

Extensive research in computer security attempts to improve existing technologies. For example, biometrics is a much safer user-access control method [Ives et al. 2004] and is relatively inexpensive to implement. Yet, its diffusion and adoption in organizational settings and for e-commerce protection is minimal. Similarly, alternative approaches to e-payments that eliminate the use of credit cards have not been adopted. Although quantum encryption was expected to replace traditional encryption, it was not yet commercially available by 2007.

Secure Software

The Trustworthy Computing Initiative (TCI) was launched by Microsoft in January 2002 (http://news.com.com/2100-1001-816880.html). The key aspects of TCI include availability, security, privacy and trust. Its goals were to:

1. Increase the availability of computer systems by reducing down time, increasing redundancy and automatic recovery, and improving a system's self-management capabilities;
2. Increase privacy by allowing users to specify policies for the use of their information;
3. Increase information systems security;
4. Gain users' trust. This last goal extends beyond security because it involves stakeholders such as component producers, partners, and developers.

Vista, developed under TCI guidelines, is claimed to be Microsoft's most secure platform to date. It contains additional security features[18] that will obsolete many third-party vendors' security software. Yet, analysts quoted in the computer trade press claim that nothing is fundamentally different in Vista to make it more secure.

The need to increase users' trust in personal computers is also recognized by other major IT vendors. For example, The Trusted Computing Platform Alliance (TCPA, formed in 1999) included nearly 200 hardware and software vendors. This consortium was formed by IBM, Microsoft Corp., Intel Corp., HP and Compaq. Its vision was to develop a set of standards that enable PCs to communicate while maintaining privacy and security. In 2003, AMD, HP, IBM, Intel and Microsoft formed the Trusted Computing Group (TCG). The group published a set of standards (similar to the TCPA's standards) for a trusted computing environment. In October 2004 Intel, IBM, and NTT DoCoMo launched the Trusted Mobile Platform (TMP) specifications.

Sample Delphi Questions

Financial Liability

Assume PROHIBITIVE means that the total penalties surpass the individual or organizational risk level (also known as "risk appetite"). For pending legislation see http://news.zdnet.com/2100-1009_22-6181330.html.

Assume the following industries: healthcare, financial and retail. Answer only for those industries that you know well. Please give your opinion by checking the appropriate year

---

[17] The variance depends on organizational size. Small organizations spend substantially more on information security than large organizations.
[18] New features include a two-way firewall, BitLocker hard drive encryption Windows Defender (which includes anti-spy ware software) Enhanced Authentication Model, User Account Control (UAC), Encrypting File System (EFS), Protected Mode for IE 7, Group Policy for Device Lockdown, Address Space Layout Randomization (ASLR), Kernel Patch Protection, and Network Access Protection. Not all features are available for all versions. Vista does not include anti-virus software (although existing third-party software did not work with Vista). Vista 64 bits edition includes Kernel Patch Protection but the 32-bits version that most home users run does not.

Industry Name	Penalties related to identity thefts become prohibitive in the U.S. by: 2010 2015 2020 2025 Never	Penalties related to identity thefts become prohibitive globally by: 2010 2015 2020 2025 Never
1.Health care	| | | |	| | | |
2.Financial	| | | |	| | | |
3.Retail	| | | |	| | | |

Please add any COMMENTS you may have that explain your answers :

Privacy Breaches

Suppose, as was the case with TJX, privacy breaches result only in minimal financial and stock price impact on a firm and, furthermore, government penalties stay the same. Should business investment in security for privacy? (circle one.)

Stop	Reduce	Stay the Same	Increase

Please give the reasons for your choice. Feel free to add comments on penalties related to privacy breaches:

Government Response

Suppose a very secure operating system for PCs can be developed. However, the development, maintenance and adoption costs are very high (assume the simplest version of the operating system sells for $750 per seat in 2007 dollars plus hidden adoption costs). Please estimate the earliest, most likely, and latest year when such a system would appear on the market and the corresponding years for each of the responses.

Note: Use " Never " as an answer where you believe the event will never occur.

Action	2010	2015	2020	>2025	Never	Other alternatives
Quantum Encryption						
Biometrics						
Fully secure (98%) O/S						
Fully secure network						
Uncontainable virus						
Society no longer relies on IT						

Event	Earliest Year	Most Likely Year	Latest Year
The $750 system described above appears on the PC market.			
U.S. government involvement forces the use of the more secure O/S by businesses.			
A global agreement is signed and ratified that mandates the use of the secure O/S internationally.			

Possibilities

For each of the following possibilities, indicate the cumulative probability of occurrence by the date given. If you believe the event will never happen, just check Never.

In addition, if you believe there are alternative ways of achieving the same end, please list alternatives in the space provided.

The table lists shorthand for the action. The following are the definition of the terms.

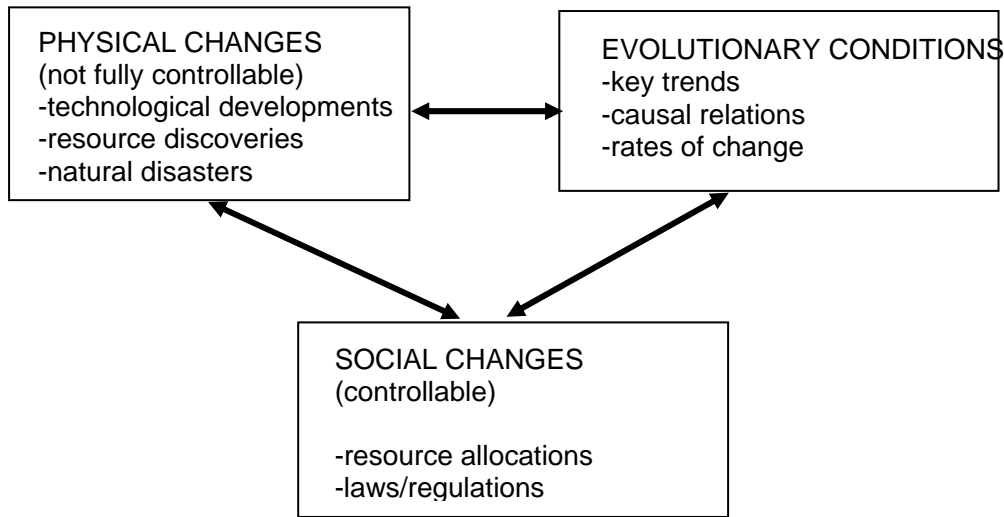1.   Quantum encryption is commercialized and replaces traditional encryption.

2. Biometrics becomes the prevalent user control mechanism.
3. The dominant operating system is 98 percent secure.
4. A fully secure network is available commercially.
5. A virus that cannot be contained in a timely manner is invented and released.
6. Society's reliance on IT declines because security becomes risky and prohibitive.

APPENDIX B. ASPECTS OF CROSS-IMPACT MODELING

In Section III we pointed out that several methods exist for performing cross-impact calculations. In this appendix we describe one of these models, INTERAX. INTERAX was developed and implemented in the late 1970s at the Center for Futures Research at the University of Southern California by a team headed by Olaf Helmer and Sel Enzer. The model is compatible with the descriptions of Section III. The model can be used in planning for:

- sensitivity studies (e.g., changes in probabilities or forecasts)
- scenario development (e.g., providing outcomes under given assumptions)
- comparative policy analysis (e.g., contingencies, actions)

Process to Determine a Future Condition

PHYSICAL CHANGES
(not fully controllable)
-technological developments
-resource discoveries
-natural disasters

EVOLUTIONARY CONDITIONS
-key trends
-causal relations
-rates of change

SOCIAL CHANGES
(controllable)

-resource allocations
-laws/regulations

The following are examples:

Physical Changes	Evolutionary Conditions	Social Changes
Global warming	Defenses against spam	Virtual worlds
End of Moore's law	Presence of Wi-Fi hot spots	Social networks
Nanotechnology	Percentage of computer literate adults	

Inputs to the Cross-Impact Study

In creating an INTERAX model, the inputs shown in Table B-1 are required.

Table B-1. Inputs to Cross-Impact Analysis	
1. A time horizon	Usually a fixed number of years, such as 10, 20, or 30
2. Potential future events	Sudden changes that have a non-negligible chance of occurring during the time horizon. Events may be one time (e.g., new invention) or recurring (e.g., major security breach).
3. Trends	Ongoing state of affairs such as number of PCs, bandwidth to home users
4. Probabilities of event occurrence	Expected over time, all other things being equal. Uses interval probabilities obtained from Delphi or other sources
5. Trend values	Anticipated over time, all other things being equal. Obtained from Delphi or other sources
6. Policy actions	Policies that may be instituted or changed
7. Interactions	Among events and trends, That is, the cross-impacts

The anticipated values of events and trends, all other things being equal, are obtained from Delphi or other sources. "All other things being equal" implies that the forecaster, implicitly or explicitly, took the impact of changes (particularly high probability events and significant trends) into account.

Sequence of Steps in Interax

Before starting the model:

1. The time horizon is divided into shorter intervals. Each interval is called a scene. The intervals need not be equal in length. Often the length of successive intervals increases in size the further into the future they go because the uncertainties increase.
2. Obtain the needed inputs listed in Table B-1.
3. Determine interval probabilities for events and interval values for trends.[19]

The analyst is now ready to use a computer simulation to generate a scenario.

Begin with the first scene and repeat for each scene thereafter.

1. For each event in the model, use a random number generator to declare whether the event occurred during the scene or not,[20]
2. Based on occurrence or non-occurrence of each event (in scene j), the model updates the probabilities of each of the events and the values of each of the trends in the next scene (j+1).
3. Move time forward to the next scene (j+1). Use the updated values from Step 2 as the current conditions for scene (j+1).
4. Repeat steps 1, 2, and 3 for each scene until reaching the end of the time period being modeled.

Input Data

Whereas in a Delphi analysis, the panel only estimates the probability of occurrence of n events over time (as shown in Table B-2), in cross-impact analysis the panel must also determine the pair-wise impacts of events on one another. Thus, for example, suppose the Delphi forecasts for the cumulative probabilities of occurrence of three events are as shown in table B-2:

Table B-2. Cumulative Probability of Occurrence over Time				
Event	2008	2011	2015	2020
A	.02	.05	.10	.15
B	.05	.30	.45	.50
C	.10	.30	.35	.37

and the values of Trend 1 (such as, energy required by a PC relative to 2007) are estimated to be:

Trend	2008	2011	2015	2020
1	105	96	80	72

The panel is asked to determine the cross impacts among the events. Because cross impacts are computed in terms of multipliers on the likelihood of occurrence(Table B-3), a cross-impact of 1 indicates no effect, values greater than 1 lead to an increase and values less than 1 lead to a decrease in likelihood of occurrence. For simplicity, we assume that there is no effect of an event on itself and assign the value 1 to self-impact in our sample of three events. Six cross impacts of events on other events are possible and a matrix is created. For example:

Table B-3 Cross Impact of Events			
	Cross impact on A	Cross Impact on B	Cross Impact on C
If Event A	1	2	3
If Event B	0.5	1	1
If Event C	1	0.25	1

---

[19] Although the Delphi outputs for events tend to be cumulative probabilities, interval probabilities (i.e., the probability in each scene) are required computationally. Converting cumulative probabilities to interval probabilities is straightforward.
[20] The random numbers are decimals between 0.0 and 1.00. For example, if the event has a 2% chance of occurring in the interval, if the random number, RN, is in the interval 0< RN <=0.02 then the event is declared to occur; if it is >0.02 the event is declared not to occur.

With three events and one trend, three event-on-trend cross impacts are also possible. For example:

	Cross-impact on Trend 1
If Event A	1.05
If Event B	1.20
If Event C	0.90

For reasons described in Appendix C, these numbers refer to the multiplier to be applied to the odds of events and the value of the trend. Note that effects need not be symmetric. In the example, if event B occurs it does not affect event C but if event C occurs it results in a major decrease on the odds of B. Such a relation, for example, would indicate that the occurrence of an innovation (such as event C) would make it much less likely that event B (e.g., development of a competing innovation) would occur.

A detailed discussion of the cross-impact matrix for events is given in Enzer [1980].

Dealing with Trends

In a cross-impact analysis, a variety of methods are used to deal with trends. There is no standard approach as yet. We describe one method here. The Delphi panel (Section II) is given historical data on a trend and is asked to forecast the value of the trend over the time horizon. This forecast is used as the input to the cross-impact analysis. Three issues need to be considered:

1. The effect of an event occurring or not occurring in a scene (say scene j) on the trend value in the next scene (j+1). For example, if the event is the development of a new "super root kit" it could affect the trend of the expenditure on security.

2. The effect of a trend on the probability of occurrence of an event. For example, a spike in the trend of R&D investment in security (in scene j) could increase the probability of new countermeasures being available in the next scene (j+1).

3. The effects of trends on one another. For example, the number of security incidents (in scene j) on the size of the IS security workforce (in scene j+1).

To take into account the random fluctuations in trends, the values of the trends can be varied stochastically. That is, in each scene, the computer creates a random change in the trend value, with small perturbations for stable trends and large perturbations for volatile trends.

APPENDIX C. THE MATHEMATICS OF UPDATING PROBABILITIES IN CROSS-IMPACT ANALYSIS

It is important to understand that cross-impact analysis involves a different treatment of probability than does either probability theory or statistics [Alter and Enzer 1978]. Probability and statistics both deal with analyzing fixed data about constant situations. In cross-impact analysis the objective is to create a systematic way to deal with changes in the forecasted probability of occurrence based on new evidence. Therefore, the model examines possible future developments and their interactions in a stochastic world rather than analyzing what was or is in a static world.
To explain the probability updating process, we use three concepts: balance, odds, and likelihood ratios.

Balance

Consider two events,

- B, which occurs with interval probability p(B(j+1)) in scene (j+1); and

- A, which occurs with interval probability P(A(j)) in the previous scene (j) and has a cross impact, XI, on B[21] .

In a simulation, we expect that the fraction of times that event B occurs in scene j+1 is equal to P(B(j+1)). However, because of the cross impact of A on B, B's probability of occurrence in scene j+1, is changed, depending on whether or not event A occurred in scene j. To maintain the property that B occurs with probability P(B(j+1)) we assume that the expected value of P(B(j+1)) will be equal to the input value. Since in cross-impact simulation A will either occur or not in period j, we can write the expected value of P(B(j+1)) as:

P(B(j+1))= P(B(j+1)|A occurred)*P(A) +P(B|A did not occur)* (1-P(A))   (C-1)

Think of Equation (C-1) as a balancing relationship. For example[22] if P(B(j+1)) = 0.6 and P(A(j))= 0.3 then

---

[21] In this example, we assume that A occurs only once and did not occur prior to scene j.

$$0.6= P(B(j+1)|A(j) \text{ occurs})*0.\,3+ P(B(j+1)|A(j) \text{ does not occur})*0.7 \qquad (C\text{-}2)$$

It will turn out that we can determine the conditional probabilities by using likelihood ratios. To do so we will need to convert probabilities to odds.

Odds

To update probabilities in a consistent manner, INTERAX uses odds [Enzer 1980]. The odds of an event occurring, in simple language, is the ratio of the number of times an event is expected to occur to the number of times it is not expected to occur. Thus, odds are related to probabilities by the relation:

$$ODDS = PROBABILITY/(1\text{-} PROBABILITY) \qquad (C\text{-}3)$$

or, solving for probability:

$$PROBABILITY = ODDS/(1+ODDS). \qquad (C\text{-}4)$$

For example, if the probability of an event in a scene is 0.6 then its odds = 0.6/0.4 = 1.5 and, conversely, if the odds are 1.5, then the probability is 1.5/2.5 = 0.6

Odds are useful because of two properties:

1. The odds are needed to compute two quantities (see below):
    a. The likelihood ratio of occurrence (LRO)
    b. The likelihood ratio of non-occurrence (LRN)
2. Multiplying odds by cross impacts leads to updated odds, which in turn leads to updated probabilities.

Likelihood Ratios

The likelihood ratio concept comes from statistics and is widely used in medicine [e.g., Simon 2007]. For example, in medicine it provides a direct estimate of how much a test result will change the odds of having a disease. The likelihood ratio for a positive result (the likelihood ratio of occurrence, or LRO) tells you how much the odds of the disease increase when a test is positive. The likelihood ratio for a negative result (likelihood ratio of non-occurrence, or LRN) tells you how much the odds of the disease decrease when a test is negative. In cross impact, LRO is the likelihood ratio of the occurrence of an event and LRN is the likelihood ratio of its non-occurrence. LRO and LRN are multipliers.

LRO is simply the cross impact of event A if it occurs in scene j on the odds of B occurring in scene j+1. Thus, if event A occurs,

New odds of B = previous odds of B *LRO = previous odds of B * cross impact

For our example, if

   (1) the event A occurs;
   (2) the cross impact of A on B is 2; and
   (3) the previous odds of B are 1.5;

then the new odds are 1.5*2 = 3. Converting the odds to probability (using Cc-5) Equation (C-4)), $P(B(j+1)|A(j)) = 3/(3+1)$. In this case the new probability P(b(j+1) is ¾ or 0.75.

In the balance relationship of Equation (C-1), the probability of 0.75 just computed is P(B|A occurs).

Equation (C-1) also provides a way of computing the probability P(B|A does not occur). Solving Equation (C-1) for this probability yields the following equation:

$$P(B(j+1)|A(j)\text{does not occur})=(P(B(j+1))- P(A(j))*P(B(j+1)|A(j) \text{ occurs}))/(1\text{-}P(A(j)))$$

---

[22] We use very large values for the interval probabilities to make it easier for readers to follow the calculation. In actual cases the interval probabilities would be much smaller.

The probability computed in the above Equation is the updated probability in scene (j+1) if A does not occur. In our example where P(B(j+1) = 0.6, P(A(j)) = 0.3, and P(B(j+1)|A(j)) = 0.75,

P(B(j+1)|A(j) does not occur) = (0.6 – 0.3*0.75)/(1-0.3) = 0.375/0.7 = 0.5357

Thus, in our example, the probability of occurrence for event B in scene j+1 increases from 0.6 to 0.75 if event A occurs in scene j and decreases to 0.5357 if event A does not occur in scene j.

We use these results to compute LRN.

For P(B|A does not occur) = 0.5357, the new odds are 0.5357/(1- .5357) =1.1538

LRN = (New odds of non-occurrence in scene (j+1)/ original odds in scene j)

   = (1.1538/1.5) = 0.769

(Check: Odds in scene j * LRN = new odds = 1.5*0.769 = 1.1538

    New probability = 1.1538/2.1538 = 0.5357)

Additional details of the probability updating process are given in Alter and Enzer [1980].

APPENDIX D. POTENTIAL PITFALLS OF FUTURES RESEARCH

Linstone [2002] lists eight pitfalls in doing and/or using futures research.   In brief these are:

1. *Discounting the future.* Linstone argues that most executives have only a short time horizon and, in effect, hope that new solutions, not currently known, will somehow arise.
2. *The prediction urge.* Making positive definite statements rather than indicating the constraints and caveats on what is found.
3. *The simplification urge.* Simplifying statements about what is found.
4. *Illusory expertise.* People may know about a specific subsystem (e.g., firewalls) but make predictions about a complete security system.
5. *Sloppy execution.* Poor selection of participants, poor iteration with participants, superficial analysis.
6. *Optimism-Pessimism Bias.* Over-optimism in short-range forecasts and over-pessimism in long-term bias.
7. *Fits all bias.* Using one or more of the methods in this tutorial for all problems, whether they apply or not.
8. *Deception.* Use deception and manipulation to achieve desired outcomes.

Other critiques of futures research exist and should be examined by potential users. Be aware, however, that some, like the one by Sackman [1971], which argues that Delphi is invalid because it does not follow the standards for questionnaires of the American Psychological Association, are now generally discredited.

ABOUT THE AUTHORS

Paul Gray is Professor Emeritus and founding chair of the School of Information Systems and Technology at Claremont Graduate University. He was the founding editor-in-chief of CAIS from 1999-2005. He is a recipient of the AIS LEO award for lifetime achievement and a Fellow of both AIS and INFORMS. He is the author of 14 books (the latest being *What They Didn't Teach You in Graduate School*) and more than 140 papers. He is currently Visiting Professor at the University of California at Irvine.

Anat Hovav teaches at Korea University Business School. She published in journals such as *Information Systems Research, Computers and Security, Communications of the ACM, ISJ, Communications of AIS, Information Systems Frontiers,* and *Information Systems Management*. Her research interests include electronic scholarship, the adoption of Internet standards, and Information Security.