The User Non-Acceptance Paradigm: INFOSEC's Dirty Little Secret. Panel

Submitter and Panel Chair/Moderator: **Victor Raskin**

Steven J. Greenwald, Independent INFOSEC Consultant

Kenneth G. Olthoff, National Security Agency

Victor Raskin, NLP & CERIAS, Purdue University

Willibald Ruch, Psychology, University of Zurich

Abstract (by Victor Raskin)

This panel will address users' perceptions and misperceptions of the risk/benefit and benefit/nuisance ratios associated with information security products, and will grope for a solution, based on the psychology of personality trait-factoring results, among other multidisciplinary approaches, to the problem of user non-acceptance of information security products. This problem has acquired a much more scientific guise when amalgamated with the psychology of personality and reinforced by reflections from the field on patterns of user behavior. A gross simplification of the main thrust of the panel is this thesis: if we start profiling the defenders rather than the offenders and do it on the basis of real science rather than very crude personality tests, then we will, at the very least, understand what is happening and possibly create a desirable profile for sysadmins, CIOs, and perhaps even CFOs. This swept-under-the-rug problem is information security's "dirty little secret." No other forum is designed to address this, and it may well become yet another major conceptual and paradigmatic shift in the field, of the type initiated in the NSPWs over the last decade. We know that the panel will generate an assured considerable interest among the participants.

1. Introduction: A Brief Pre-History (by Victor Raskin)

After a brief pre-history and a reasonably calm review of the problem ("our dirty little secret"), I will synthesize Willi(bald Ruch)'s and my own views on the subject and then present the views of Ken (Olthoff) and Steve (Greenwald), from those horses' mouths (I think I got the horse end right in this idiom).

A couple of years ago, I submitted a paper to the workshop on the issue of user non-acceptance. My proposed solution (which I will later briefly reiterate as part of the panel body) was to bribe the sysadmin into installing an InfoSec software package by bundling with it an intelligent humor agent that would entertain him or her in the process and beyond. The submission was praised and rejected because the complaint, with which I completely agreed, was that there was much more on computational humor in the paper than on security. There was, however, a bit of a Catch-22 situation here: there could be no pertinent body of knowledge in InfoSec on this unless we had an opportunity to talk about it.

The current situation has changed in two important respects. First, we have talked much more about it, and valuable InfoSec-related insights have been and are being added to that body of knowledge, coming from established figures in the field, NSPW veterans, and other recognized authorities. Second, a bunch of us sought out and brought on board a leading psychologist of personality (Willibald Ruch), who can and will put our commonsense ideas on how to (begin to) handle the problem on a sound scientific foundation.

2. Our Dirty Little Secret? Nobody Loves Us: The Users' Boycott (by Victor Raskin)

An army of talented mathematicians, computer scientists, and engineers has been proposing one elegant scientific solution after another to a host of technical problems in InfoSec for decades. These often have an application-independent scientific value. They constitute the bulk, if not the entirety, of the most prestigious conferences' activities. A bunch of hopeful entrepreneurs has been working on commercializing these solutions into nifty software packages. Some enthusiastic and farsighted (or trusting and stupid?) CEO's have purchased the packages. A much larger cohort of CIOs and sysadmins have cheerfully reported on the installation of these products. So how come Purdue University, the proud home of the Center for Education and Research in Information Assurance and Security (CERIAS), provides basically no protection to its networks' Microsoft Windows users and is routinely blacklisted by Earthlink, Juno, and other InfoSec bastions (my tongue is lightly touching the inside of my cheek right now) for relaying spam and viruses? The answer to that *is* our dirty little secret. Surely some packages are not so good and the hackers can also overpower just about any good package. But amazingly, many products are never even installed, or uninstalled shortly after the initial installation and configuration process because of the performance penalties that result. And nobody's head is on the line.

In the even less favorable case, an organization does not purchase any InfoSec package at all, seeing a form of insurance in it and deciding that it is as unaffordable as other forms of insurance that a company has decided to forfeit at its own risk. At an entrepreneurs' panel at the CERIAS Fourth Annual

NSPW 2004 Nova Scotia Canada

Research Symposium (2003), an experienced participant identified CFO's—responsible ones at that—as the main stumbling block on the road to creating a more secure environment: they are not hired to make an investment that will not contribute positively to the stockholders' dividends. If we are a form of insurance (cf. Blakley et al. 2002) then it is a cause of alarm because we lack the industry's established presence, its experience in making customers buy its products whether needed or not, its penetration of governments' legislative and legal establishments, let alone the highly seductive, romantic, and witty image of a State Farm insurance agent (T-in-C again, but you know what I mean!). The general discussion in the panel has revealed different opinions about the relations between security and insurance: some believed that the insurance market might encourage the acceptance of InfoSec packages by rewarding it with lower premiums. Others were much less enthusiastic about the market's effectiveness.

The invited plenary speaker at the CERIAS Fifth Annual Research Symposium (2004), a pleasant, quick and glib mechanical engineer (oops, an oxymoron here?), a CMU graduate (oh, okay then), recently appointed to head InfoSec at the U.S. Department of Homeland Security (a position apparently downgraded once from Deputy Secretary to deter Richard Clark, twice to lose Howard Schmidt, and twice more just in case), was asked whether, in his opinion, the market forces were failing InfoSec. His answer was, essentially, that, first, they were not failing, second, they will stop doing that during his tenure, and, third, in any case the government should not do anything to interfere with market forces. Rejoicing in the fact that he will go far in politics, we should make a real effort to make a crack at the problem because if anybody counted on his help before, please don't anymore! [He has since also resigned.]

At the 2003 NSTAC at Atlanta last spring, I added this problem to the list of issues identified in one of the discussion strands, where it was put in the context of whether security should be made invisible or transparent in any software, a topic likely to be raised during the discussion portion of this panel. (The guest of honor, that very Richard Clark, then still the chair of the President's Cyber Security Council, mentioned this problem by name in his concluding remarks. As he delivered that list to the President, he promptly resigned from the Council, and his successor, Howard Schmidt, with whom be briefly discussed it at that 2003 CERIAS Symposium, promptly followed suit.)

These issues overlap with general software usability concerns, and this is where the NSPWs have so far come the closest to the non-acceptance problem (see, for instance, Rannenberg 2001—cf. Müller and Rannenberg 1999; Brostoff and Sasse 2002—cf. Reason 1990, Anderson 2001, Whitten and Tygar 1999). Surely, the more usable the product and attractive the interface, the more customer acceptance. But the remaining point, typically not addressed, is one of the several that occupy us here: will the best usability in the world overcome the (perception or even misperception of) performance penalty imposed on the secured system?

3. The Psychology of Personality, Computational Humor, and Other Multidisciplinary Research of User Non-Acceptance (by Victor Raskin, as enlightened on the first issue by Willibald Ruch)

While technical research in InfoSec focuses on how to protect computer networks and files, the recent multidisciplinary effort, pioneered by CERIAS some 5 years ago and greatly encouraged by the government, largely through the designation of Centers of Academic Excellence by the NSA, tries to view InfoSec in its entire complexity. But even there, the emphasis has been largely the study of the attacker and of attack anticipation, prevention, and recovery.

The psychology of personality, the discipline never yet directly involved in the multidisciplinary effort, offers us a continually upgraded view of human trait clustering. These incredibly well-designed experiments take human subjects with an established personality trait and test them for a number of other traits, using reasonable-level statistics to establish reliable correlations, positive or negative. The psychology of personality disdains the existing personality tests as outdated and distorting—though I think that we must accept the reality and utility of their wide acceptance as a tool, crude as it may be, and, in fact, subsequent to an e-mail solicitation, a paper based on one of those tests and dealing with one aspect of the problem in hand is likely to be submitted to the Workshop.

In a world-famous experiment, Ruch and associates tested the hypothesis that people of right-wing views had no sense of humor while their ideological opponents did. While confirmed on the O'Reilly/O'Franken comparison, the hypothesis will work, in the real-life research it did not pan out, but a subtler correlation emerged: the right wingers favor sexual humor while the left wingers are much more receptive of absurd humor. Replicated in a number of countries, this research has led to the creation of 3WD (see Ruch 1998 and references there), the widely accepted and possibly best sense-of-humor test. To dispose of humor yet within this paragraph, I proposed, on the basis of my own formal semantic theory of verbal humor (psychologically justified in collaboration with Ruch—Ruch et al. 1993) and, subsequently, computational humor (see Raskin 2002), to include the humor intelligent agent, developed by us, on a European Union grant to the University of Twente in Holland (Dr. Anton Nijholt—see Nijholt 2002) and the Italian Institute of Research in Science and Technology (Dr. Oliviero Stock) for different applications (Stock and Strapparava 2002), in the InfoSec software bundle to bribe the sysadmins into installing the packages and entertain them in the process.

In the course of a recent meeting between Willi and a few of us, on our way back from NSPW 2003 last August, sensation-seeking emerged immediately from Willi's prior, InfoSec-unrelated research as a trait clearly inimical to InfoSec. This is when the discussion turned to defender profiling as the most promising solution to the non-acceptance factor: a sensation-seeker is a risk taker, so he/she will not buy an InfoSec software package; if bought by somebody else, they will not install it; if forced to install, they will use the first customer complaint about a performance deficit as an excuse to uninstall it.

We also talked about the legality of defender profiling in the process of job interviews, and this is where the psychology of personality can help greatly: given that many questions cannot be asked for legal and ethical reasons, the discipline may offer a number of innocent-sounding members of the same cluster as the substitute. While I cannot ask a prospective candidate for a sysadmin job whether he or she is an irresponsible risk taker, I can ask them, over a beer, whether the idea of ski or bungee jumping has any appeal to them, and the affirmative answer will establish the candidate as a sensation seeker and, therefore, a risk taker. Willi and his group are still working on how to detect, behind my effervescent façade, an obsessive paranoid type compulsively buying every insurance product as it comes on the market (my demise will certainly bring the industry down, as every company pays out twice its equity to my lucky heir).

A subsequent discussion on SecurityPsych, the mailing list set up by Ken in August 2003 for discussing the non-acceptance issues, has broadened the area of application of the psychology of personality to profiling defender supporters, such as lobbyists and even legislators. There are, obviously, problems with immediate implementations of such projects but it is very important, I think, to face these sociopolitical issues up front, especially when/because they (under)cut the much better defined and developed technical aspects of InfoSec as well as undermining their many successes.

4. Breaking the Problem Down Into Boxes (by Kenneth G. Olthoff)

The following categorization scheme is offered as a very rough start at breaking the problem of user non-acceptance into various subsets. This is an initial attempt to separate out the various factors that might be in play, so that approaches to those factors may be considered independently for corrective action. It is assumed that in any given situation several of the factors below might apply and interact, and that the categories may not be mutually exclusive in all cases. It is also acknowledged that this conceptual framework is merely a starting point for further discussion and research, and by no means the last word on the subject. Any suggestions for restructuring or expansion of the categories presented would be welcomed.

Please note that we are only addressing user non-acceptance. The analysis of the factors and incentives that might lead users to cooperate with the use of a tool (whether the tool is appropriate for the context or not) is a related issue that will not be addressed in this paper.

It seems that no matter which factors apply, there are two main aspects to a thorough analysis. First is developing an understanding of the factual circumstances - the "real" situation, including all influences, incentives, and penalties. The second is to develop an understanding of the user's perceptions, which may be highly colored by misunderstandings, biases, communication difficulties, hidden agendas, and other factors. Both the factual and the perceptual issues must be addressed if one is to optimize the level of user acceptance.

To generalize (or perhaps stereotype), technologists tend to direct more energy to analyzing the factual aspect of the problem space. The perceptual (sometimes derisively termed "touchy-feely") aspects are often dismissed as being in the "soft sciences", or presumed to not be of concern to engineers and computer scientists. It is interesting to note, however, the number of entries in the categorization below that are unrelated to the specifics of the tool. While technologists tend to focus on the interesting aspects of technology, this categorization points out that there are many other issues that require our attention, independent of technical issues.

Even aside from the normal "human factors" and "user friendliness" issues, the categorization highlights issues such as the relationship of the user to the organization, the common understanding of terms and concepts, the degree to which the individual's mental model and values match those of the organization, and the incentive/disincentive structures surrounding the use of the tool, none of which are likely to be solved by strictly technological means. This may argue for a more multi-disciplinary and holistic approach to security than has been typical (admittedly with exceptions) up to this point.

When reading the following, assume that the word "tool" may apply to a security mechanism included as apart of a larger system such as an encryption option within an application, a security procedure, a security system that is a "stand alone" device such as a firewall or intrusion detection system, or any other security related artifact. Assume that the word "user" applies to any human who is affected by or interacts with the tool (or decisions about the purchase or use of the tool) at any level of the system, including end users, system administrators, system integrators choosing products to integrate into a larger system, corporate/organizational decision makers, etc. With those definitions in mind, let us proceed to the categorization.

The categorization has been laid out in rough chronological order as one would go through the process of choosing and implementing a tool. It provides a structure in which to think about the various problems, though some specific types of problems may in reality emerge in multiple phases in the timeline.

Categories one and two cover issues that may come up when the organization is first contemplating whether they need the tool or not.

Category three comes into play once the decision to use a tool has been made, and deals with the trade-offs (real or perceived) between performance and risk.

Categories four, five and six address the point in the process when the implementers and user community are presented with the information that the tool is going to be installed. These categories deal with resistance based on the concept of the tool, the authority under which the tool is being mandated, and concerns about how the tool might change the status quo. All three of these categories may become factors before anybody actually tries to install the tool.

Category seven deals with the users' understanding of the tool itself, and the attempts to install it.

Categories eight and nine deal with the sort of issues that might arise as one attempts to configure the tool and discovers that the process of doing so brings to light problems outside of the tool, or mismatches between the tool and the target environment.

Category ten assumes that the tool has finally been set up to run, and deals with the effect of the interaction between the tool and the environment in actual use.

4.1 MISUNDERSTOOD OR MISAPPLIED RISK/REWARD

4.1.1
The user assumes that security is unnecessary, for whatever reason - "Nobody is attacking my system!" or "I don't have anything of value to lose or hide"

4.1.2
The user miscalculates the degree of risk, and therefore makes an inaccurate or inappropriate cost/benefit judgment.

4.1.3
The user optimizes risk locally or for personal or local benefit, rather than at a larger network, organizational, or global level. Game theory might play heavily into this.

4.1.4
The potential enabling functions of the tool are not presented or not understood. The user is not aware of what increased functionality might be possible with the tool in place that would not be possible without it. The user doesn't understand "what's in it for me".

4.2 LIABILITY/RESPONSIBILITY IMPOSED OR IMPLIED BY TOOL USAGE

4.2.1
The use of the tool would make the user officially aware of problems, thus giving the user the task of fixing them - ignorance is bliss, but it may also allow one to duck responsibility!

4.2.2
The use of the tool may introduce tort liability. For example, depending on the legal or regulatory model in a particular jurisdiction, if you don't take any action related to security and tell your customers that, you might in some instances abdicate responsibility, but if you try to operate securely and fail, you may be held accountable for the inadequacy of your efforts. Another legal model might say that the failure to use the tool may be seen as a lack of due diligence, so this argument can go both ways, depending on the specifics and the laws or regulations within a particular jurisdiction.

4.2.3
The rules in varying jurisdictions (the U.S., the various states within the U.S., the EU and its component countries, etc.) may conflict or mandate a contradictory combination of constraints, thus forcing the user into the worst of all possible worlds in order to be compliant, if compliance across all relevant jurisdictions is even possible.

4.2.4
The user ("user" being defined at any level) may be basing her behavior on fear of being punished, complicated by the fact that the user's understanding of the laws or regulations may or may not be accurate. In other words, the user chooses nonacceptance of the tool, in pursuit of compliance with her understanding of other laws or regulations she deems to have overriding jurisdiction.

4.3 PERFORMANCE vs. RISK DECISIONS

4.3.1
The user perceives that security mechanisms or procedures exact a performance penalty and is unable or unwilling to accept the penalty. This gets into issues of how one balances a documented performance cost against the potential loss from a security incident.

4.3.1.1
The perception is accurate – there is a performance penalty of the magnitude perceived.

4.3.1.2
The perception is inaccurate.

4.3.1.2.1
The user never tries the tool long enough for the inaccurate perception to be proved wrong.

4.3.1.2.2
The perception is inaccurate, but becomes a self-fulfilling prophesy – the user hasn't checked the "before" performance closely, and only assumes that the "after" numbers represent a significant decrease that is attributed to the tool.

4.3.2
The user views security and performance as directly opposing factors, rather than seeing them as relating in some other way, and makes the risk/performance tradeoff or optimization based on mistaken assumptions about the relationship, interaction and correlation of the two factors.

4.4 THE USER HAS CONCEPTUAL CONFLICTS WITH THE TOOL

4.4.1
The user has philosophical or ideological objections to the tool, the policy, or the desired results - "Down with Big Brother (or The Manufacturer, or whatever)!" "Information wants to be free!" etc.

4.4.2
Individual user's mental model of security does not map to that of the tool (or the organization), and the user exhibits the "wrong" behavior, even when trying to do the "right" thing.

4.5 THE USER HAS CONFLICTS WITH AUTHORITY

4.5.1
The user's problem is not with the tool, but with those who are mandating the tool.

4.5.1.1
The user does not acknowledge or respect the authority of those mandating the tool. "Those people in <America, the EU, the Computer Industry, the Sysadmin shop, Corporate Headquarters, other> can't tell *me* what to do!!!"

4.5.1.2
The user does not respect the judgment or expertise of those mandating the tool. "Those people don't know what they are doing!"

4.5.1.3
The user does not trust those who are mandating the tool

"I don't know what they are really up to with this tool, but I'm suspicious of them."

4.5.2
The tool is mandated or presented in an unattractive way, rather than presented in such a way as to stimulate in the user a desire to comply out of enlightened self-interest, altruism, ethics, patriotism, or other "virtue".

4.5.3
The user perceives the mandated use of a tool in general, or the specific action of the tool, to be a personal affront. The user sees the tool as an indication of mistrust on the part of the system owners, a comment on the person's ability to act correctly without supervision, etc.

4.6 AVOIDANCE OF DETECTION AND THE CLOSING OF HOLES

4.6.1
The tool, if used correctly, would highlight unauthorized behavior on the part of the user that the user would prefer to not be detected. Note that this item does not assume a value judgment on the unauthorized activity or presume that the activity is harmful or illegal. It need only be something the user prefers to not be discovered. We presume in this case that the tool will disclose the unauthorized activity, presumably to somebody in authority who had previously been unaware of the unauthorized activity.

4.6.2
The tool might close down unauthorized or undetected "alternative uses" of the system that the user has grown accustomed to. The user knows that the back door or the playground is being shut down, and chooses not to cooperate. In the previous case, the user feared detection, while in this case, it is the loss of covert functionality that is the issue. We assume here that the unofficial activity will merely be prevented by the tool, not disclosed.

4.6.2.1
The unofficial usage is a positive one that benefits the organization, perhaps actually increasing productivity or otherwise improving performance.

4.6.2.2
The unofficial usage is relatively harmless, perhaps including pastimes such as games, office romances, joke mailing lists, announcements of unofficial employee activities such as sports leagues, etc.

4.6.2.3
The unofficial usage is negative, perhaps including acts that actively harm the organization or violate regulations and laws.

4.7 THE TOOL'S DESIGN IS ALIENATING OR CONFUSING TO THE USER

4.7.1
The language used within the tool, the policy, or the documentation is poorly chosen, and elicits an avoidable negative reaction on the part of the user.

4.7.2
The user doesn't understand how to install/configure/use the tool.

4.7.2.1
The user doesn't even try, believing the task to be beyond his abilities.

4.7.2.2
The user tries, grows frustrated, and gives up.

4.7.3
The user misunderstands how to install/configure/use the tool. In this case, the user tries and succeeds, but gets it wrong somehow - the tool works, but is inappropriately applied to the circumstances.

4.7.4
The user misunderstands the purpose of the tool. In 7.2, the user knows what the tool is supposed to do, but sets it up incorrectly. In this case, the user attempts in good faith to use the tool to do something that it is not designed to do, believing the tool's proper function or capability to be something other than it really is.

4.8 THE TOOL HIGHLIGHTS OTHER PROBLEMS

4.8.1
The policies or security goals of the system prior to the introduction of the tool are internally inconsistent, thus making it impossible to configure the tool successfully. Humans adapt (often without realizing it, or at best on an ad hoc basis) to the rule/policy inconsistencies in non-automated systems, but computers can only follow the rules they are given. Thus, the introduction of an automated tool sometimes brings incongruities to light, even though the incongruities have already been present previously.

4.8.2
The use of the tool reveals security problems or incidents that have already occurred (finding back doors in one's system, detecting fraud or theft, etc.), leading to confusion, retribution, or cover-up.

4.9 USE OF THE WRONG TOOL FOR THE TASK

4.9.1
The model/policies/assumptions supported by the tool don't map well to the target environment, making acceptance or use of the tool difficult or impossible.

4.9.2
The tool prevents, prohibits, or hinders necessary actions, either because of inability to isolate the risk-inducing actions from those that are essential, or because the essential actions *are* inherently risk-inducing.

4.9.3
The user (at whatever level) knows the tool itself or the chosen configuration of the tool is inappropriate for the context. This condition may have the side effect of not only increasing frustration with the tool, but reducing respect for and cooperation with those who chose and implemented the wrong tool or configuration.

4.10 INTEROPERABILITY ISSUES

4.10.1

The tool conflicts with other parts of the user's system, in ways that are ancillary to the primary security function of the tool. For example, the tool might use too many resources, and thus prevent other parts of the system from operating correctly.

4.10.2

The tool conflicts with other parts of the system in ways related to the tool's function. For example, the tool might shut down a port, or interpose itself as a proxy in a data flow that another piece of the system depends on.

4.10.3

The tool assumes or requires a configuration of the system that necessitates modifying the existing architecture or procedures. Even when the required configuration changes or modifications make no substantive change in system operation, there may be resistance because "we've never done it that way before".

5. Information Security Breeds User Insecurity and Non-Acceptance: A Contrarian View (by Steven J. Greenwald)

5.1 Introduction

I take a contrarian position for this panel in the interests of a contentious (and therefore interesting) panel, among other valid reasons that I hope to make clear. And after all, given enough time and research dollars can't we all prove anything we want? Anything at all?[1]

I submit the following as a thesis: *Users perceive they have too much Information Security on their systems and that is why they are psychologically resistant to add even more Information Security*.

Now, I didn't believe my thesis at first. After all, it flies in the face of party doctrine and in the old days we would be put up against the wall if we uttered something similar. But after some research I came to the conclusion the thesis is actually correct! Of course, some will say that my powers of rationalization are truly astonishing.

Of particular interest is an integration into this thesis of Hagbard Celine's Laws of Chaos, Discord, and Confusion.[2] Celine's Laws were invented after "the accumulation of three decade's worth of careful metasociological research" in preparation for Celine's three-volume study, *Why Everybody Is Going Bonkers*.[3] According to Celine himself:

> Here I can only mention the thousands of depth interviews, the innumerable flowcharts and helix-matrix equations, the vast files of computer readouts, the *I Ching* divinations, and the other rigorous scientific techniques used in developing what I modestly call Celine's Laws of Chaos, Discord, and Confusion.[4]

I propose that we can modify Celine's Laws for usage in the Information Security field, and that these modifications are quite effective in describing the reasons for user non-acceptance.

A lively discussion resulted during the presentation of this section that was recorded by the tireless NSPW Scribe, Bob Blakley. Rather than totally rewrite this section to incorporates the discussion input and ideas, it is untouched, except for this paragraph, and an epilog that incorporates some of the outstanding discussion areas. I hope that this conveys some of the flavor of the NSPW process for those readers not fortunate enough to have attended.

5.2 Celine's First Law

A modification of Celine's First Law ("National Security is the chief cause of national insecurity" often paraphrased as "Anyone who isn't paranoid must be crazy") is quite interesting. For the purposes of user acceptance of Information Security we can modify it as "Information Security begets user insecurity" which I think is what is happening right now.

As a current example, I quote from a recent Associated Press article, *Microsoft Expands Windows Update Release*.[5] This article is about Microsoft's (by the time this appears in print I conjecture) infamous Service Pack 2 (SP2) update.

> With only a small percentage of users running the product, analysts say they aren't seeing any unexpected problems so far. But some expect confusion to mount as more people begin installing the update.
>
> "Microsoft realized that a lot of people are going to have some level of problems, no matter how good a job they did with it," said Steve Kleynhans, a vice president with META Group, based in Stamford, Conn. "When you start tweaking with Security ... you're bound to break applications. It's always been true and it always will be true."

It is important to note here that Microsoft's humongous Service Pack 2 update is solely concerned with Information Security. Also of note is Mr. Kleynhans' apocalyptic and chilling absolutism on the issue.

So here we have a not-so-little example of how Information Security begets user insecurity. What sane user would want to take the enormous time to download[6] and then install SP2 absent a clear reason for doing so (such as an obvious Information Security problem that is actually affecting them as opposed to, say, a nebulous Distributed Denial of Service attack problem that the average user can't even comprehend)? And then, once SP2 is installed, users can expect it to perturb the applications in their systems (this is a common effect of

---

[1] I beg the reader's forgiveness for my abandonment of my usually stuffy scholarly style—this is, after all, a panel on the use of humor for user (non)acceptance. Still, I am deadly serious about my thesis.

[2] Celine's (1980).

[3] Not yet published, as far as I can determine. *N.B.* that Celine is as tenacious as Donald Knuth though.

[4] See the reference before the previous one, page 118.

[5] Linn (2004).

[6] For a user with a 56Kbps dialup modem, the approximately 60 megabyte SP2 update will take at least 2 hours and 23 minutes to download under optimum conditions (and conditions are never optimum). Installation will take longer of course.

patches, and a major reason to reject the "penetrate and patch" paradigm, but that has been discussed to death elsewhere).

Of course, some would argue the opposite (*i.e.*, that it is the lack of Information Security that begets insecurity) but I argue against this, since in those halcyon days of early PCs and the ARPAnet there was no Information Security at all and no user worried about it overmuch.

Clearly we must come to the conclusion that there is a strong correlation between an increase in Information Security awareness and Information Security problems. Coincidence? I don't think so! A causal link remains to be proven and I will gratefully accept grant money for further research in this area.

5.3 Celine's Second Law

Celine's Second Law is also of interest due to Microsoft being in the equation ("Accurate communication is only possible in a nonpunishing situation" which was derived, I think, from a statement that Freud made ("That which is objectively repressed (unspeakable) soon becomes subjectively repressed (unthinkable)")). Or as Celine said, "It is easier to cease to notice when the official reality grid differs from sensed experience" (which I think Celine stole from Korzybski by the way, but as this is just a panel I am too lazy to actually look it up in Count Korzybski's massive tomes, *Science and Sanity* and *General Semantics*).

Basically, the average user implements this law by never disagreeing with the boss overmuch. In that sense, Microsoft has excellent Information Security. In fact, its Information Security is so excellent that there is too much of it, so enough already!

Do you think I am being facetious? Then consider that most users believe that Bill Gates is a genius, and Microsoft is the leader in software technology, *ad nauseam*, despite (and I cannot stress this enough) *their own direct experience with Microsoft garbage and problems!* So from the average user's viewpoint there is no Information Security problem whatsoever! Forget acceptance! It is like trying to make a person stuffed with food eat even more (actually it is worse than that, but proper decorum limits me).

There are some interesting ramifications from this regarding B.F. Skinner's random reinforcement of behavior (*e.g.*, Microsoft's patches) and how that leads to crazy behavior (*e.g.*, users continuing to buy Microsoft products). Perhaps Bill Gates *is* a genius, but only in the field of psychology/marketing.

5.4 Celine's Third Law

Celine's third law is also worth examination ("An honest politician is a national calamity") since it would seem that the *zeitgeist* of the panel audience (indeed, the INFOSEC community in general) is that there should be some sort of action at the highest levels to cram Information Security down the throats of those who are too unaccepting of its benefits (someone correct me if I am too presumptuous and uncharitable here). In that sense, Celine has clearly documented the absolute horrors that are caused by honest politicians (briefly: dishonest politicians are interested in only enriching themselves at the public expense, which is a goal shared by most of their fellow citizens; an honest politician is committed to bettering society by political action and therefore screws things up by enacting more laws - the assumption is that adding more laws is a positive achievement when history has surely proven the opposite since each new law creates a new criminal class, *e.g.*, illegalizing marijuana in the U.S. in 1937 created hundreds of thousands of criminals).

Regarding this panel, Celine's Third Law can best be expressed as, "Be careful what you wish for; you might get it." Now think about this: do we *really* want users demanding good Information Security? If you think so, then please consider the following ramifications. While it has been commonly accepted (and I have propounded this view in my past ignorance and also because I am a good capitalist) that only user demand will cause the marketplace to develop Information Security solutions, the great flaw in this argument is that it presupposes that there *are* any good Information Security solutions at the present level of technology! What will we say as crowds of irate users are lynching us since we cannot provide them with what we have told them they need and want? King Canute could not possibly have placed himself in a worse position than we have, as we try to turn back the tide of technological inadequacy, but instead provide (in the immortal words of Marv Schaefer) "Band-Aids™ and dilute iodine along with pixie-dust!"

There is an interesting side-argument here about economics—about how there is no such thing as a consumer without producers, and so forth, but I will leave that argument to the Objectivists. Basically: the idea that Information Security must be consumer driven is clearly insane, since economics is obviously driven by production, and not consumption. This is a basic economic axiom. If you doubt this then think about how importing several million consumers to an ailing country's economy would only make matters worse, while importing an equal number of producers could not fail to cause a great benefit. Also consider the "brain drain" effect and how that was instrumental in the destruction of such economies as the Soviet Empire's. However, since (mercifully) I am not an economist, I will refrain from further comment, since there is no one so ignorant as an expert outside his own field. I refer the interested reader to the writings of Ayn Rand[7] (in particular, her essay collection, *Philosophy: Who Needs It*[8]). I also advise the reader to avoid anything written by John Maynard Keynes, who had a penchant for getting things precisely reversed.

5.5 Conclusion

As my research continues I have a growing and horrifying suspicion that my thesis is correct. In particular I have noticed the following (each as an example of the three laws, respectively -- and I could have provided a huge amount of examples if I had wished!).

1. Microsoft's Service Pack 2.
2. From a recent SANS article: "Microsoft will make available $1 million as a request for proposal to develop secure computing curricula in computer science, business and law. Microsoft also announced a $1 million New Faculty Fellowship program which will award five $200,000 fellowships to 'exceptional new computer

[7] No relation to the Rand Corporation.

[8] Rand (1982). In particular Essay 12, "Egalitarianism and Inflation," pp. 120—136.

science faculty members.'"[9] Upon examination, the curriculum required is entirely Microsoft-centric.

3. The U.S. Transportation Security Agency. Enough said.

If you agree with my thesis, then welcome to the club! If you disagree with it, then you can use it as an interesting argument *ad absurdum* . Either way, I think debate and examination of this subject is long overdue.

6. Epilog

(As I mentioned in the introduction, I decided to leave the original of this section untouched, except for the inclusion of this epilog (and the mention of it in the introduction to this section). This should help give the reader a glimpse into the NSPW process, as well as allow a before-and-after comparison without any loss or modification of the original material. It also more easily allows attribution of some of the comments by the workshop participants. Also, while Bob Blakley did (as usual!) an outstanding job as the NSPW Scribe, I do not want to inadvertently put words in people's mouths, so please view the attributed remarks as paraphrases of the original comments by the attributed persons. Any mistakes are solely mine. What follows is some of the discussion for my part of the panel.

Gerry Allwein asked if I really meant that we are responsible for *all* user insecurity. I answered, "Yes!" In my view we clearly are responsible for all user insecurity regarding information security. If we did not exist, then users, *ipso facto* could not feel insecure without themselves becoming, in some sense, information security people themselves (I phrased this a little differently *in situ*). Bob accused me of using Jesuit trickery at that point (with some justification on his part, I must admit). Gerry then pointed out that users are clearly aware of viruses, so how are *we* making the insecure? I responded by saying that we tell them to install virus checkers, but they usually don't install them until they get a virus. The result is that security professionals are blamed because we told people about viruses in the first place (the basic "kill the messenger" effect).

Michael Franz asserted that many users love viruses because getting a virus means the problems aren't their fault. This is analogous to "the dog at my homework" defense that students sometimes use. If so, this would be orthogonal to my position. Sometimes even the worst situations are capable of having some good effects.

Konstantin ??? gave the excellent analogy of cancer: before we knew about cancer, people just died. But that didn't mean physicians *created* cancer; they just discovered it. True enough, however, I believe that once physicians discovered cancer, people started having anxiety about it. Consider how many people put off having preventative diagnostic procedures (such as mammograms) because they are afraid of getting bad news.

Michael Franz wanted me to distinguish random errors from exploitable vulnerabilities. This is certainly a valid point, but I think random errors are outside the scope of my position. Michael asked Bill Gates how many Chinese agents he thought were working for Microsoft and were maliciously inserting vulnerabilities. Mr. Gates said, "That's not our problem; that's the government's problem." My response to that was "I'll get to that (in my presentation; which I hope I did). I then mentioned that at the present time I thought it was bad policy to disagree with Bill Gates. Bob replied, "Just ask Dan Geer!" Jeremy mentioned as an example a quote from a fifth grader: "What was it like before Bill Gates invented the computer?"

Brian Snow cited a book titled *Toxic Leadership*, and mentioned that the issue is that users see no *actionable* problems; it isn't that they don't see problems. I disagreed and referred back to Freud's quote. Brian replied that he thought that Freud used "unthinkable" in a stronger sense (*i.e.*, as literally unthinkable) than they way to which I was referring. Maybe so, but I think the point is still valid. Bob agreed with Brian that this may be the case for home users, but mentioned that things are *really* unthinkable for corporate users.

Gerry Allwein asked if what I'm really observing is not repression, but instead fear of change. I replied that this may be true, and cited B. F. Skinner on random reinforcement schedules. Basically, if subjects are randomly reinforced, the resultant behavior appears totally crazy (or consider how gamblers become addicted to things like slot machines). Gerry then pointed out that a lot of issues may stem from products breaking when security (or anything else) is installed. Users don't recognize that it is because the software underneath is brittle. And *we* told them to install the stuff so of course *we* get blamed!

Bob then asked why Galileo's cantilever beam experiment didn't cause well-engineered beams to fail. The reason is that well-engineered beams (at least in Galileo's time) were designed empirically. The prevailing theory at that time was faulty, as Galileo showed. At present, we don't have well-engineered empirically correct security systems (although we have plenty of theory). It is interesting to note that Galileo's discovery that the breaking force on a beam increases as the square of its length was, in essence, the discovery of a scaling problem. If any engineer who was a contemporary of Galileo had used the old method (*e.g.*, to double the load that a beam must carry then just double the dimensions of the beam) it would have led to catastrophic failure (and perhaps it did).

Abe Singer then made an analogy to Eugene M. Shoemaker's theory of catastrophic asteroid impacts[10]. Before that, only a few science fiction writers and science fiction readers worried about the possibility of highly destructive asteroid or meteor impacts.

Konstantin Beznosov asked what we can learn from other, more mature, fields. Victor Raskin answered the question by saying that I was obviously wrong (talk about non-acceptance!) but I was still evocative, as paradoxes are supposed to be. Victor, I strenuously disagree that my position is even a paradox, although semantics aside, I understand (and affectionately disagree with) your point.

John McHugh referred to a talk he used to give called "Faith and Hope: Methodologies for Building Trusted Systems." He cited an example of a client who was afraid to install an effective security guard technology because they thought

[9] "Microsoft Announces $1 Million for Secure Computing Curriculum Development," SANS NewsBites (Vol. 6 Num. 34), August 2, 2004 available at <http://www.infoworld.com/article/04/08/02/HNmscurricula_1.html>

[10] Shoemaker (1960), Shoemaker and Kieffer (1974).

doing so would be an admission that the system the guard was supposed to protect was insecure.

John also talked about economic free-riding (people with the ability to protect the system but with no incentive to do so). John also talked about another economic problem: that the cost of risk is large in the aggregate but too small per individual entity to create incentives to fix the problem. Put another way, we are dealing with distributed economics: while a virus might cost $X billion, it is not clear how much of that is any individual (or organization's) portion. The damage is spread so thin that we don't worry about the economic impact to us He concluded by wondering if we need a bigger disaster. I'm afraid I must agree with John on this; it is unfortunate that we seem, at present, to be reactive when it comes to information security.

Abe Singer then cited insurance companies as risk mitigation drivers. Brian Snow cited an insurer who added a 15% premium to business continuity policies issued to customers looking for damage recovery insurance who ran Microsoft software on servers; Brian felt that this was a generally good idea. Bob replied that insurance won't work for two reasons. First, pooling does not work economically for correlated cases, which attackers can create deliberately (*i.e.*, worms); in other words, we are not dealing with stochastic events, but with intentional events. Second, analog systems' failure modes can be exhausted (except for a very unlikely statistical "tail") by a finite number of observed failures, whereas software evidently has an *infinite* supply of failures which have never previous been experienced (*e.g.*, patching never ends); so refusing insurance for having known vulnerabilities does not actually reduce the aggregate risk (*i.e.*, we can't know that a certain level of security has ever been obtained). However, Jeremy Epstein noted that the insurance example was a publicity stunt; there was no way to determine if 15% was even the right amount. Brian then noted that insurance companies are throwing software liability back onto vendors, which, as John McHugh observed, finally *does* place the economic incentive to fix the problem with the correct party.

7. References

[1] Anderson, R. J. 2001. Security Engineering: a Guide to Building Dependable Distributed Systems. New York: Wiley.

[2] Blakley, B. (G. R. III), E. McDermott, and D. Geer 2002. Information Security Is Risk Management. In: V. Raskin and C. F. Hempelmann (eds.), Proceedings. New Security Paradigms Workshop 2001. September 10th-13th, Cloudcroft, NM, USA. New York: ACM Press, 97-104.

[3] Brostoff, S. and M. A. Sasse 2002. Safe and Sound: A Safety-Critical Approach to Security. In: V. Raskin and C. F. Hempelmann (eds.), Proceedings. New Security Paradigm Workshop 2001. September 10th-13th, Cloudcroft, NM, USA, New York: ACM Press, 41-50.

[4] Celine's Laws, 1997. Celine's Laws of Chaos, Discord, and Confusion. In: R. A. Wilson (ed.), The Illuminati Papers, Berkeley, CA: Ronin, 118-125.

[5] Linn, A. 2004. Microsoft Expands Windows Update Release, August 25.

[6] Müller, G., and K. Rannenberg (eds.) 1999. Multilateral Security in Communications. Munich: Addison-Wesley-Longman.

[7] Nijholt, A. 2002. Embodied Agents: A New Impetus to Humor Research. In: Stock et al., 101-111.

[8] A. Rand 1982. Philosophy: Who Needs It. New York: Signet.

[9] Rannenberg, K. 2001. Multilateral Security: A Concept and Examples for Balanced Security. In: M. Schaefer (ed.), New Security Paradigm Workshop. September 18th-22nd, 2000. Ballycotton, County Cork, Ireland, New York: ACM Press, 151-162.

[10] Raskin, V. 2002. Computational Humor and Ontological Semantics. In: Stock et al., 31-46.

[11] Reason, J. 1990. Human Error. Cambridge: Cambridge University Press.

[12] Ruch, W. (ed.) 1998. The Sense of Humor. In: V. Raskin and W. Ruch (eds.), Humor Research Series, Vol. 3. Berlin: Mouton de Gruyter.

[13] Ruch, W., S. Attardo, and V. Raskin 1993. Toward an Empirical Verification of the General Theory of Verbal Humor. *Humor: International Journal of Humor Research* 6:2, 123-136/

[14] Shoemaker, E. M. 1960. Penetration mechanics of high velocity meteorites, illustrated by Meteor Crater, Arizona, Internat. Geol. Conf, 21st Session, pt. 18, Copenhagen, pp. 418-434.

[15] Shoemaker, E. M., and S. W. Kieffer 1974. Guidebook to the Geology of Meteor Crater, Arizona. 37th Annual Meeting of the Meteoritical Society, August 7, 1974. Reprinted in 1988 by Center for Meteorite Studies, Arizona State University, Tempe, Arizona as Publication No. 17.

[16] Stock, O., and C. Strapparava 2002. Humorous Agent for Humorous Acronyms: The HAHAcronym Project. In: Stock et al., 125-135.

[17] Stock, O., C. Strapparava, and A. Nijholt (eds.) 2002. The April Fools' Day Workshop on Computational Humor, April 2002, ITC-irst, Trento. TWLT 20: Twente Workshop on Language Technology. European Project IST-2000-30039. Enschede, NL: University of Twente.

[18] Whitten, A., and J. D. Tygar 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, Washington, D.C., August.