Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Measuring Psychological Variables of Control In Information Security

The effects of an individual's personal feelings of control over aspects of their health have been well studied in the field of Medical Psychology. However, these variables have not been explored in the field of Information Security. If these variables have the same impact within Information Security as they do within Medical Psychology, it could indicate that current practices such as locking down users' workstations are counterproductive. This paper proposes a method of measuring the variables of Actual ...

Copyright SANS Institute
Author Retains Full Rights

AD

Measuring Psychological Variables Of Control In Information Security

GIAC (GSLC) Gold Certification

Author: Josh More, jmore@starmind.org
Advisor: Carlos Cid

Accepted: 10 January 2011

Abstract

The effects of an individual's personal feelings of control over aspects of their health have been well studied in the field of Medical Psychology. However, these variables have not been explored in the field of Information Security. If these variables have the same impact within Information Security as they do within Medical Psychology, it could indicate that current practices such as locking down users' workstations are counterproductive. This paper proposes a method of measuring the variables of Actual Control, Perceived Control and Vicarious Perceived Control and engages in an analysis of sampled data. The initial results are promising with regards to the psychological measurements, though adjustment variables did not have the expected results. Determining the full impact of these variables on organizational security will require additional work to measure the damage that security incidents cause.

© 2011 SANS Institute, Author retains full rights.

Introduction

"Perceived Control" is a core construct used in the psychology field that can be considered an aspect of empowerment (Eklund, & Backstrom, 2006). Effectively, it is a measure of how much control people feel that they have, as opposed to the amount of "Actual Control" that they may have. It is often paired against constructs such as "Vicarious Control" and "Vicarious Perceived Control", which measure the amount of control that outside entities have over the subject. Often, these are variables measured in the psychology/health field. For example, in the world of medicine, when patients report a lack of perceived control over controllable illnesses such as diabetes (Helgeson, & Franzen, 1997), breast cancer (Helgeson, 1992) and heart disease (Helgeson, 1992), they often do more poorly than patients who feel that they have a greater sense of control over their illness. There is also evidence that students with high perceived control do substantially better academically than those with low, though this seems to also link with emotions surrounding the tasks at hand (Ruthig, Perry, Hladkyj, Hall, & Pekrun, 2008). In short, people who are interested in and excited by what they are doing tend to perform better.

The operating theory is that if a medical practitioner can serve to increase the feelings of perceived control within their patients, the negative effects of their illness may be lessened. It must be noted, however, that the positive effects of perceived control only seem to exist in situations where the subject/patient can actually improve their condition through their own efforts and that perceived control is far from alone in its impact on negative effects (Wallston, Wallston, Smith, & Dobbins, 1987). In the case of illnesses such as AIDS that progress regardless of patient actions, perceived control is not a positive benefit (Helgeson, 1992) .

It has also been observed that the greater the actual threat, the greater the value that perceived control can play. In the health field, this is often explored as control over disease vs control over symptoms. For some diseases, such as rheumatoid arthritis, control is helpful with pain management, but has not been proven to slow the progress of the disease itself (Helgeson, 1992).

The practice of using biological concepts to model events within computer and

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

network systems is very common. Malicious software is often discussed in terms of small biological pests such as viruses and worms. Interconnected systems have been found to have nascent emergent behavior like neural networks (Hopfield, 1982). While they are not necessarily a complete match to reality, these analogies have proven to be useful within the information technology fields both in understanding complex systems and drafting strategies to better manage them.

Therefore, this paper proposes a system of measurement to determine the amount of perceived control that exists in common corporate workplaces, positing that people and their computers function as a single "organism". It would be expected that an operator's feeling of control over their endpoint would serve to reduce some risks but not others. To maximize the benefit of perceived control in the workplace, one would hope for strong feelings of perceived control in situations where the user can act to reduce large threats, and low feelings of perceived control in situations where their actions would not have a positive impact on their risks.

Measurements and Modifiers of Control

Model Overview

The model in use throughout this research is that users and computers, together, serve as a mutual feedback system. In other words, the user inputs data to the computer, which responds with data, to which the user responds with more data. Clearly, this is not as tightly an integrated system as the human body alone, where numerous sensory organs feed input to the brain, but it might be more comparable to a single-celled organism that interacts with its environment strictly through the sense of touch.

In this model, there are two primary sources of variables. Internal variables would measure the interaction between the user and their workstation. External variables would measure the interaction between the user/workstation “organization” and their environment of other user/workstation pairs, departments (commonly, the security department) and the organization/company as a whole. Since the focus of this paper is on control, these variables will come down to control of workstation by the user and control of the user or workstation by a department or the organization itself.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

If this model is correct, one could then draw on common findings from the psychological fields and apply them to security policies as they are enforced within an organization. This could allow for a security department to more accurately project the way that users might respond to technical controls and improve the efficacy of those controls. It is hoped that this could also serve to reduce the tensions that often exist between the common attitudes of "security is there to protect us" and "security just gets in our way".

Dimensions of Control

One fundamental difficulty with measuring psychological variables is that unlike the more technical disciplines, there is a higher inherent level of uncertainty. This uncertainty extends both to the measurements themselves, but also to what is being measured. Psychology is still an emerging science, and there is disagreement as to which variables are truly orthogonal and which are simply subsets of other variables. It is impossible to be either complete or precise in these measurements.

In order to maximize the usefulness of this research, the focus here is on "translating" the existing discussion from Psychology to Information Security. To keep the translation as simple as possible and thereby make the conclusions drawn by Psychologists most useful to Security Architects, Analysts and Engineers, the focus of this paper narrows on a handful of variables, how they may be measured and what existing Psychological research indicates that certain measurements may mean.

This section introduces the specific variables being considered.

Actual Control

In a nutshell, a person with actual control is capable of changing their circumstances through their own actions. For example, if a person is facing the risk of breaking their arm falling off a ladder, they experience actual control over the situation by having choices to mitigate those risks. They could tie the ladder to the roof, double-check the positioning pre-climb, avoid stepping on the top-most step, etc.

In a less trivial example, home computer users often experience high levels of actual control over their risk exposure. They can choose which websites to visit, whether to open email attachments and whether to apply system updates. In contrast, many

© 2011 SANS Institute, Author retains full rights.
© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

computer users experience low actual control within their workplaces. Technologies such as web filtering, antimalware and patch management have control over systems and therefore reduce the amount of control that users experience.

Perceived Control

Perceived control is the level of control that people perceive themselves to have. In the area of heart health, it has been shown that high levels of perceived control correlate to better health than those with low levels of perceived control (Helgeson, 1992). It is important to note, however, that perceived control only seems to provide an improvement to one's risk posture if it is in areas where the individual also has a high degree of actual control (Helgeson, 1992).

In our world, one would expect that users with low perceived control over many security risks would be seen in environments with tighter corporate security controls. This is reasonable, as they also have lower actual control in these environments. In environments with less mandated controls (nonprofit organizations, for example) users would be expected to report a higher level of perceived control.

Vicarious Actual Control

This variable represents the complement of an individual's actual control. In other words, it measures that amount of actual control that outside entities have over an individual. One would expect these two measurements to always add up to the same base number (assuming normalization), however it must be stressed that this will only happen if there is only a single entity that has control over the subject. This may seldom be the case. It would also normalize poorly if there were an area of shared control, such as a technology used by an IT department that could manage a system, but that could be disabled or bypassed by a user.

Vicarious Perceived Control

Much as vicarious actual control measures that amount of control that outside entities have, vicarious perceived control measures the amount of control that outside entities are perceived to have. One might expect this variable to have minimal effect on actual risk, however, it has been observed that people tend to increase their level of risk in response to the use of risk-mitigation strategies (Schneier, 2008).

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

This concept, known as a "risk thermostat" (Adams, 1996), is the more popular name for risk compensation theory and suggests that, among other things, people engage in impromptu risk analysis as part of their daily lives. They become comfortable with a certain level of risk, and if risks are reduced , they will often alter their behavior to raise their level of perceived risk to what they find acceptable. Because in everyday life, risks can result in both losses and rewards, a person may alter their behavior to maximize their changes of rewards while minimizing their potential losses. This works fine for personal decision making, but in situations where the person taking the risks experiences the rewards but someone else (a company, perhaps) could experience the losses, the risk thermostats may not balance the way that all parties would prefer.

Thus, if the research by psychologists is accurate and can be extrapolated to our field, the worrisome conclusion is that the higher the level of vicarious perceived control, the more risks users will take.

Realistic and Unrealistic Perceived Control

It has also been observed that the benefits of perceived control are only present where the perceived control is realistic. In other words, if an individual has had a limb removed by forcible means and is several hours from civilization, a high feeling of perceived control would likely be unrealistic and would be unhelpful in that situation. In contrast, if an individual has a family history of treatable cancer, a high feeling of perceived control could well lead the individual to seek proactive testing, engage in more frequent exercise and better eating habits.

To avoid over-complicating the model, the assumption was made that the realism of perceived control can be ascertained by careful selection of the survey questions and analyzing perceived control versus the other control variables. As such, it is not measured directly.

Symptom and Problem Control

In the medical field, there tend to be several approaches to treating illness. One is to simply address the symptoms. This treatment is usually considered in situations where the core issue cannot be treated effectively. Often referred to as palliative care, it is used in quality of life situations where the patient's feelings of comfort are considered to

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

outweigh slowing the progression of the disease. In contrast, control over the problem would focus on techniques that would cure the patient.

Extrapolating to our field, it is the difference between, for example, preventing the theft of data and preventing the damage that the data theft could cause. If an organization implements a data loss prevention system that looks for sensitive data leaving the environment and blocking it, they are exhibiting problem control. If, instead, they encrypt all laptops so that if one is stolen it is unlikely to cause damage, they are exhibiting symptom control.

As with measuring the realism of control methods, the strategy taken for this paper as to whether controls focus on the problem or the symptom is handled in the survey generation stage and this control is not directly measured.

Risk Perceptions and Expertise

The work of Du et al. has found that the accuracy of an individual's perception of risk increases with experience (Du, Keil, Mathiassen, Shen, & Tiwana, 2006). This should come as no surprise, as the longer one works in a field, the more data they have to draw upon when making projections and estimates. Clearly, accurately measuring "expertise" is just as difficult to measuring "control". However, in an attempt to correct for any inaccuracies originating from an individual's lack of expertise, the survey will include a rough experience measurement.

The Survey Method to Measure Psychological Variables

We are extremely fortunate to be in the Information Security field. Most of our technical systems generate data; lots and lots of data. Sometimes, they generate inordinately high and unmanageable quantities of data. We can analyze data directly (by looking for something or the absence of something) or indirectly (by combining data sets and using inference). We even have enough data that we can analyze it statistically and look for patterns that we might not otherwise know about.

Other disciplines are not as lucky. In Physics, Chemistry and Biology, you may have to measure things like mass, length and temperature. These quantities may not be what we actually want to measure, but they are discrete and objective. It may take more

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

work, but we can generally uncover the actual information we care about.

However, when you are measuring variables surrounding people, you inevitably face measuring the subjective. Sadly, humans do not (yet) have a port in their skulls that you can plug into and download the information you care about. Instead, all information must be filtered through a constantly changing and inconsistent neural network. While some interesting work is being done using direct measurements, most practical information must come from the people themselves. As Helgeson does in her work (Helgeson, & Franzen, 1997), (Helgeson, 1992) and as it is common in other psychological studies (Beckjord, Glinder, Langrock, & Compas, 2009) and (Ruthig, Perry, Hladkyj, Hall, & Pekrun, 2008), the easiest way to obtain this information is to simply ask them. Thus, surveys will be used, naturally resulting in something of a less ordered data set.

Surveys and "Good Enough" Data

There are numerous techniques that are typically used to make this data more reliable. Most of them, however, are beyond the scope of this paper. This sort of research is iterative in nature. As flaws are found in one survey, they are corrected in the next. Fortunately, unless the research question is particularly specific the data is usually "good enough" to draw reasonable conclusions. However, if you are accustomed to reading technical analyses where every measurement has a low threshold of uncertainty and can be traced back to a specific technical process, this process will seem somewhat loose.

One technique used to limit inaccuracy is to limit the scope of the survey. This may seem counterintuitive to the more technical disciplines, as generally, the more data you have the more accurate your results may be. However, humans are not like computers in that they tend to suffer from fatigue. The longer a survey is, the less accurate the results nearer the end tend to be (Kasunic, 2005). If the survey is kept short, the more willing people are to complete it and the more accurate the final results can be.

Likert Scales

A Likert scale is a survey method whereby individuals are presented with a series of statements and mark how closely each statement matches their experience. The results

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

of these statements are added together to get a general estimate of what value to assign to a specific variable.

After reviewing options, it was decided that the preferred survey model would be to use four level Likert items. This method is known as "forced-choice" because it prevents the survey taker from selecting "Neither agree nor disagree". The concern is that having that option could skew the data towards the center as it is easier for individuals to select the middle choice rather than considering which option best fits.

Generally, several questions are developed for each variable and are phrased both negatively and positively. When it comes time for analysis, the negatively phrased answers have their values flipped prior to being combined with other Likert items. While this is a standard method used in psychological research, it is still relatively unfamiliar within Information Security. Thus, an example may help:

If you are attempting to determine how happy a person is, you don't just want to ask "How happy are you" and ask them to mark 1 through 10, as it is impossible to know where a single person places their happiness floor and ceiling. One person may consider 1 to indicate suicidal depression, whereas another may simple consider 1 to indicate a moderate not-happy and not-sad state. Similarly, a 10 could indicate someone having a good day or someone winning the lottery on their wedding night.

Instead, one tends to get better results by removing choice and giving specific examples to those being surveyed. For example, a person would likely experience happiness in certain situations and experience a lack of happiness in others. To create a Likert scale, one generates a list of these situations:

- Getting married (positive)
- Getting shot (negative)
- Watching a sunrise with a loved one (generally positive)
- Being let go from work (generally negative)
- Finding a penny (somewhat positive)
- Getting cut off in traffic (somewhat negative)

Clearly, there are some circumstances where what is generally positive (watching a sunrise) could be negative for a particular person (who may have allergies and dislikes

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

being outside). Thus, you ask the same question several times and sum up the data. Thus, the scale itself would look like this.

I would feel happy if..	Disagree	Somewhat Disagree	Somewhat Agree	Agree
I got married	1	2	3	4
I got shot	1	2	3	4
I watched a sunrise with my loved one	1	2	3	4
I was let go from work	1	2	3	4
I find a penny on the sidewalk	1	2	3	4
I got cut off in traffic	1	2	3	4

Then, if the individual filled out the form as follows:

I would feel happy if..	Disagree	Somewhat Disagree	Somewhat Agree	Agree
I got married	1	2	3	**4**
I got shot	**1**	2	3	4
I watched a sunrise with my loved one	1	2	3	**4**
I was let go from work	1	**2**	3	4
I find a penny on the sidewalk	1	2	**3**	4
I got cut off in traffic	1	**2**	3	4

The negative items would be flipped:

I would feel happy if..	Disagree	Somewhat Disagree	Somewhat Agree	Agree
I got married	1	2	3	**4**
I didn't get shot	1	2	3	**4**
I watched a sunrise with my loved one	1	2	3	**4**
I wasn't let go from work	1	2	**3**	4
I find a penny on the sidewalk	1	2	**3**	4
I didn't get cut off in traffic	1	2	**3**	4

Thus, the person would be assigned a happiness score of 4+4+4+3+3+3 = 21.

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

By doing this, the concerns over assigning a numerical value without units are somewhat alleviated. Yes, having a happiness score of 21 on its own is meaningless, but if the average across a large set of people is 21 and a particular person measures 12, then there is a clear difference. In the psychological world, this simplistic example would indicate the presence of depression, self loathing, or a general hatred of marriage.

In our field, this analysis will allow for a score to be assigned to specific individuals and (more importantly) organizations to determine how much control different companies and departments allow their employees vs how much control those employees believe themselves to have.

Qualification

When medical professionals engage in surveys to gather data, they often have more qualifying data than the average I.T. or security professional. In order to make up for this lack of data, some questions must exist that allow the analysis phase to arrange responses or eliminate those that could skew the results for the question at hand. While it would be nice, over time, to be able to qualify many different respondents, the current fundamental question focuses on how "normal" users and security administrators perceive control in their environments. Thus, the ability to distinguish between these roles is essential.

As part of my standard duties	Disagree	Somewhat Disagree	Somewhat Agree	Agree
I respond to issues that are likely security threats	1	2	3	4
I respond to requests from customers	1	2	3	4
I define policy for my coworkers to follow	1	2	3	4
I enter data into our core systems	1	2	3	4

On this scale, reversing the dark rows, a low score of 4 would indicate an individual with job duties outside of the security realm, while a score of 16 would indicate a likely security practitioner. While scores in the midrange are certainly possible, this allows for the analysis process to set a threshold of "security responsibility" to split the data set.

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Analysis Data: Demographics

Often, patterns will emerge as data is analyzed along demographic lines. In the case of medical practice, disease can trend with race, ethnicity or sex, though the presence of socioeconomic factors that are also present along these lines may skew the data. Similarly, in the case of psychological studies, the web of links between biases related to privilege, sexism, racism and the like can be very difficult to untangle.

Since it is often unknown what patterns along these lines may arise, requesting basic demographic data can allow the future analysis to adjust for patterns that may not be directly related to the variables being studied. Unlike the rest of the survey, these questions do not form a Likert scale. Demographics questions do not require verification, and this is not a Likert scale, so there are no inverted rows in this table.

The questions in this section are optional, but will assist the researchers in analyzing your responses.				
How old are you?	15-24	25-34	35-54	54+
What is your biological sex?	M	F	It's Complex	Prefer not to answer
What is your gender?	M	F	It's Complex	Prefer not to answer
What is your highest education level achieved?	High School	College	Professional	Doctorate
Do you consider yourself...	Introvert	Extrovert	Neither	Both
How many employees are in your organization?	1-10	11-99	100-249	249+
How would you describe your organization?	Privately owned	Publicly owned	Nonprofit organization	Government
How many hours per week do you tend to work?	0-10	10-30	30-50	50+

Variable: Actual Control

Actual control measures what individuals are actually able to do as opposed to what they think they are able to do. These questions are specific to distinguish themselves from the more general questions that appear in the **Variable: Perceived Control** section. This scale does not utilize inverted rows as this value should generally correlate against vicarious actual control, which should be measured through the administrators of an organization.

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

If I wished to do so, I could	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Reboot my workstation when it's running poorly	1	2	3	4
Install the latest game on my workstation	1	2	3	4
Install the Google or Yahoo toolbar into my browser	1	2	3	4
Change the colors of my desktop	1	2	3	4
Access pornography and gambling websites	1	2	3	4
Reinstall Windows or Linux on my workstation	1	2	3	4
Disable or remove my antivirus program	1	2	3	4
Install Windows and Adobe updates	1	2	3	4

Variable: Perceived Control

Drawing from the work of Helgeson (Helgeson, 1992), and Du (Du, Keil, Mathiassen, Shen, & Tiwana, 2006), measuring perceived control within the workplace would likely focus on what activities they feel that they can perform on their company-issue workstation. To simplify the study, the basic assumption of one employee having a single non-mobile workstation is in force. Organizations that allow employees to remove laptops from the organization, use personal laptops on the network and connect personal devices to employer-provided workstations are out of scope for this study. Narrowing on these types of organizations would be an excellent exploration area for future research. This scale does not utilize inverted rows as this value should generally correlate against vicarious perceived control, as described in the next section.

I feel that I am allowed to	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Turn my workstation off and on when I wish	1	2	3	4
Install the applications I wish	1	2	3	4
Load plugins to my applications	1	2	3	4
Customize my workstation's look and feel to suit me	1	2	3	4
Browse to the websites I wish	1	2	3	4
Utilize my workstation in whatever way I wish	1	2	3	4
Disable software when I think is causing problems	1	2	3	4
Apply updates to my workstation	1	2	3	4

Just as patients must interact their medical professionals to maintain their health, computer users often must interact with the technical professionals to maintain the health of their organization. The questions below focus on how much control individuals have over this aspect of the relationship between themselves and their workstation.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

I feel that I have the ability to	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Request assistance with my workstation as needed	1	2	3	4
Receive assistance in a timely manner	1	2	3	4
Choose which support person I work with on an issue	1	2	3	4
Schedule maintenance at a convenient time for me	1	2	3	4

Variable: Vicarious Perceived Control

While similar on the surface to the questions used for actual and perceived control, vicarious controls are the reverse. These are measurements of how much control an outside entity may have over an individual. While the number of possible outside entities is vast, they have been limited to a handful of common roles within business: department manager, business owner and government, where "government" is intended to measure control via regulations as opposed to the more personal control of managers or vision of business owners.

My manager prevents me from	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Installing the applications I need	1	2	3	4
Customizing my workstation's look and feel	1	2	3	4
Browsing to the websites I need to do my work	1	2	3	4
Browsing to the websites I want to visit on my breaks	1	2	3	4
Removing software that I think is causing problems	1	2	3	4
Accessing my workstation from home	1	2	3	4
Accessing my data from home	1	2	3	4
Seeing certain types of data (credit cards, health, etc)	1	2	3	4
Copying certain types of data (credit cards, health, etc)	1	2	3	4

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

The owner(s) of my business prevent(s) me from	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Installing the applications I need	1	2	3	4
Customizing my workstation's look and feel	1	2	3	4
Browsing to the websites I need to do my work	1	2	3	4
Browsing to the websites I want to visit on my breaks	1	2	3	4
Removing software that I think is causing problems	1	2	3	4
Accessing my workstation from home	1	2	3	4
Accessing my data from home	1	2	3	4
Seeing certain types of data (credit cards, health, etc)	1	2	3	4
Copying certain types of data (credit cards, health, etc)	1	2	3	4

The government prevents me from	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Installing the applications I need	1	2	3	4
Customizing my workstation's look and feel	1	2	3	4
Browsing to the websites I need to do my work	1	2	3	4
Browsing to the websites I want to visit on my breaks	1	2	3	4
Removing software that I think is causing problems	1	2	3	4
Accessing my workstation from home	1	2	3	4
Accessing my data from home	1	2	3	4
Seeing certain types of data (credit cards, health, etc)	1	2	3	4
Copying certain types of data (credit cards, health, etc)	1	2	3	4

Adjustment Variable: Expertise

As mentioned earlier, expertise has been identified as a modifier for the accuracy of self-assessment. It is not expected that expertise would serve as as strong a modifier unless the expertise is in the same general field. Thus, the questions attempt to narrow down expertise.

With respect to my current job	Years	Years	Years	Years
I have been working in a similar role for ___ years	0-1	2-4	5-9	10+
I had a prior career doing something different for ___ years	0-1	2-4	5-9	10+

Data from this table will be converted into values as follows, with the prior career counting as half-experience:

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

With respect to my current job				
I have been working in a similar role for ___ years	1	2	3	4
I had a prior career doing something different for ___ years	.5	1	1.5	2

Thus, an individual with 10 years of experience in their current role and three years of experience in a past unrelated role would be counted as 4 (10+ current) plus 1 (2-4 year normal score of two divided by two), resulting in a total experience score of 5.

Adjustment Variable: Personal Sense of Risk

It is possible that some individuals take greater precautions when using their system due to how much risk they perceive they are incurring as a part of their daily work. If this is the case, the measurement of control must be corrected for. The following questions are adapted from the Ways of Coping Checklist, Revised 1985 (Folkman, Lazarus, Dunkel-Schetter, DeLongis, & Gruen, 1986) .To reduce the complexity of this survey, each of the common measurements used on the checklist were reworked and reduced to two questions each. The sub-methods of coping are indicated with footnotes. The superscript marks will not appear on the user-facing questionnaire. This should provide sufficient data for adjusting of control variables and might uncover interesting patterns for future research. However, this variable is likely insufficient to measure a personal sense of risk on its own.

Additionally, it is possible that a higher degree of perceived control can serve to reduce anxiety and indecision (Weinstein, Healy, & Ender, 2002). The related use of problem-focused coping mechanisms can provide a counterbalance to analysis paralysis. Problem-focused coping skills often replace emotional ones, so that behaviors like distancing themselves from those perceived as causing stress are replaced with more rational analysis and consulting experts (Weinstein, Healy, & Ender, 2002). In other words, individuals with a heightened sense of personal control may well be more likely to request assistance from the IT Security team than those who feel that the team has a high level of control over their actions.

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

When the Security team makes a change that I think is wrong or overly burdensome, I	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Stand my ground and fight for what I want [1]	1	2	3	4
Work around them [1]	1	2	3	4
Go on as if nothing had happened [2]	1	2	3	4
Didn't let it get to me and tried not to think about it [2]	1	2	3	4
Tried to keep my feeling to myself [3]	1	2	3	4
Tried to see things from their point of view [3]	1	2	3	4
Talked to someone to find out more information [4]	1	2	3	4
Talked to someone for advice on how to handle it [4]	1	2	3	4
Realized that I brought the problem on myself [5]	1	2	3	4
Accepted that this is how things have to be [5]	1	2	3	4
Had fantasies/wishes about how things might change [6]	1	2	3	4
Took it out on other people [6]	1	2	3	4
Made a plan and followed it [7]	1	2	3	4
Came up with different solutions to the problem [7]	1	2	3	4
Came out of the experience better than I was [8]	1	2	3	4
Was inspired to do something creative [8]	1	2	3	4

[1] Confrontive Coping
[2] Distancing
[3] Self Controlling
[4] Seeking social support
[5] Accepting responsibility
[6] Escape-Avoidance
[7] Planful problem-solving
[8] Positive reappraisal

Adjustment Variable: Recent Past

It is possible that a recent security event could have raised awareness and changed a user's perceptions of the control that they have over their system. This adjustment variable corrects for recent events that may otherwise skew the primary data. At the same time, it allows for the collection of data touching on the damage of security attacks. It must be noted that, as this survey is aimed at end-users, it is to be expected that they do not have the complete estimate of loss, so questions relating to damage must be considered “Perceived Damage” and not “Actual Damage” in any future analysis.

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

The following threat is a major concern in my environment:	Disagree	Somewhat Disagree	Somewhat Agree	Agree
Malware (virus) infection on my workstation	1	2	3	4
Malware (virus) infection on a server that I use	1	2	3	4
Loss of email service	1	2	3	4
Loss of web browsing	1	2	3	4
Loss of access to the company's website	1	2	3	4
Loss of access to the company's intranet	1	2	3	4
Company data stolen by an outsider attacker	1	2	3	4
Company data stolen by one of my coworkers	1	2	3	4

I have experienced a security threat that impacted my ability to do my job:	Disagree	Somewhat Disagree	Somewhat Agree	Agree
In the past two years	1	2	3	4
In the past year	1	2	3	4
In the past six months	1	2	3	4
In the past month	1	2	3	4
In the past week	1	2	3	4
Today	1	2	3	4

Due to security issues, I have lost ____ days of work	Days	Days	Days	Days
In the past two years	0-1	2-4	4-9	10+
In the past year	0-1	2-4	4-9	10+
In the past six months	0-1	2-4	4-9	10+
In the past month	0-1	2-4	4-9	10+
In the past week	0-1	2-4	4-9	10+
Today	0-1	2-4	4-9	10+

The deployment of a security technology has impacted my ability to do my job	Disagree	Somewhat Disagree	Somewhat Agree	Agree
In the past two years	1	2	3	4
In the past year	1	2	3	4
In the past six months	1	2	3	4
In the past month	1	2	3	4
In the past week	1	2	3	4
Today	1	2	3	4

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Due to the deployment of a security technology, I have lost ____ days of work	Days	Days	Days	Days
In the past two years	0-1	2-4	4-9	10+
In the past year	0-1	2-4	4-9	10+
In the past six months	0-1	2-4	4-9	10+
In the past month	0-1	2-4	4-9	10+
In the past week	0-1	2-4	4-9	10+
Today	0-1	2-4	4-9	10+

To account for the tendency for events to lose their impact over time, these variables are not summed directly, but use a simple scaling function. Impacts from six months ago are divided by two. From one year, by four, and from two years by eight. For example, if someone were to answer the table as follows:

I have experienced a security threat that impacted my ability to do my job:	Disagree	Somewhat Disagree	Somewhat Agree	Agree
In the past two years	1	2	3	**4**
In the past year	1	2	3	**4**
In the past six months	1	2	**3**	4
In the past month	1	**2**	3	4
In the past week	**1**	2	3	4
Today	**1**	2	3	4

The data would be summed as follows: 1+1+2+3*0.5+4*0.25+4*0.125, resulting in a total value of 7 as opposed to 15 which an unscaled Likert variable would indicate.

Survey Analysis

The survey was sent to a mix of user types and company sizes. It was promoted on security-focused mailing lists, technical mailing lists and social media sites. It is expected that this will self-select for the more technically-adept, but should be sufficient to gather general trending data. There were a total of 46 respondents, though four were eliminated for incomplete or inconsistent responses. The remaining 42 were graphed with all three measures of control against the various variables discussed earlier in this paper.

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

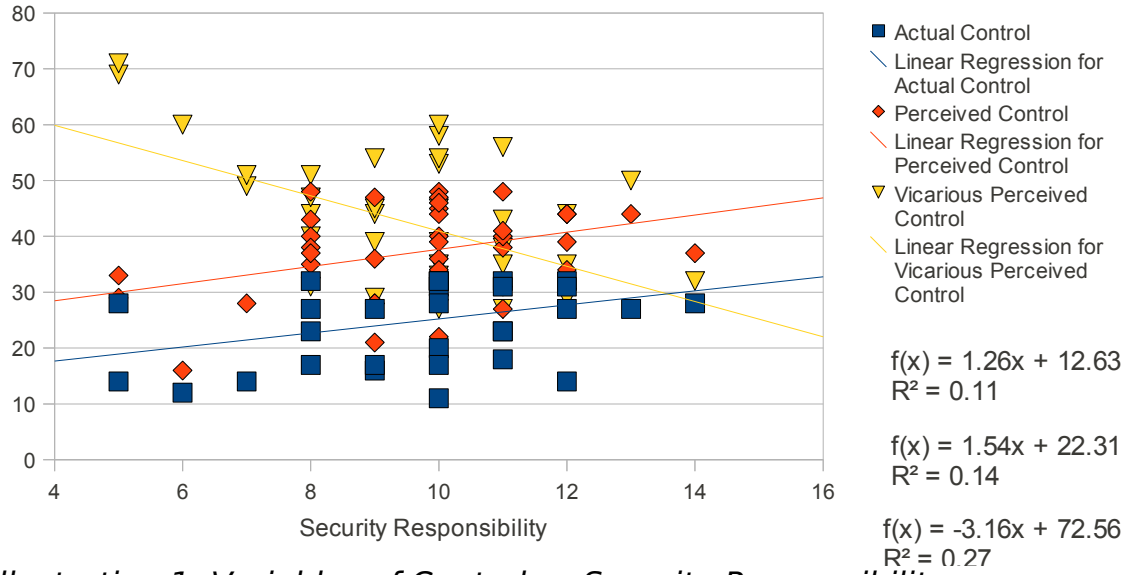

Illustration 1: Variables of Control vs Security Responsibility

The strongest trending was, as expected, in the comparison between a person's responsibility for security and how much control that person has over their environment. It is reasonable to expect that as one's responsibility for security rises, their level of control and perceived level of control rise. Similarly, the control that others have over them decrease.

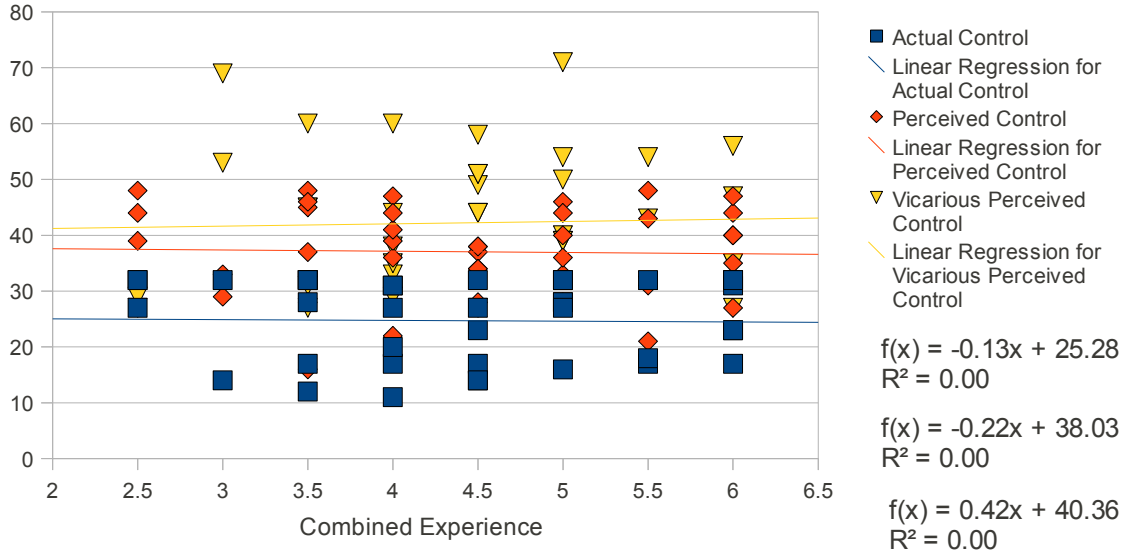

Illustration 2: Variables of Control vs Combined Experience

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Surprisingly, there does not seem to be any substantial trending of a person's feelings of control with respect to the amount of job experience they possess. It was expected that actual control would trend very slightly upwards with experience, but in our experiments, this was not the case.

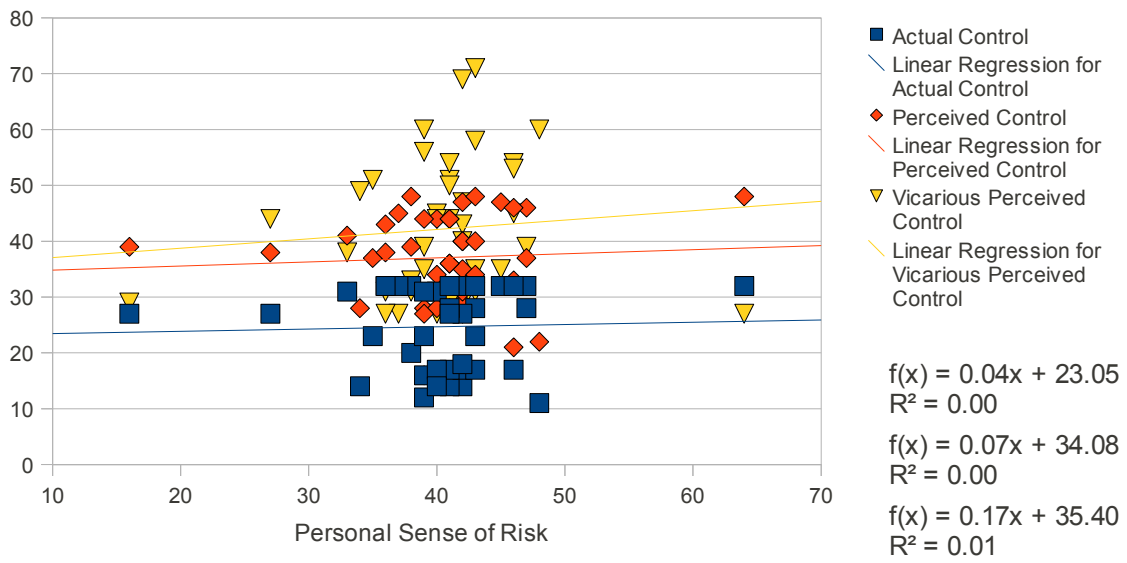

Illustration 3: Variables of Control vs Personal Sense of Risk

As expected, as an individual's personal sense of risk increases, so does their perception of vicarious control. It is reasonable to expect that in situations where perceived risk is higher, organizations will exert a greater amount of control.

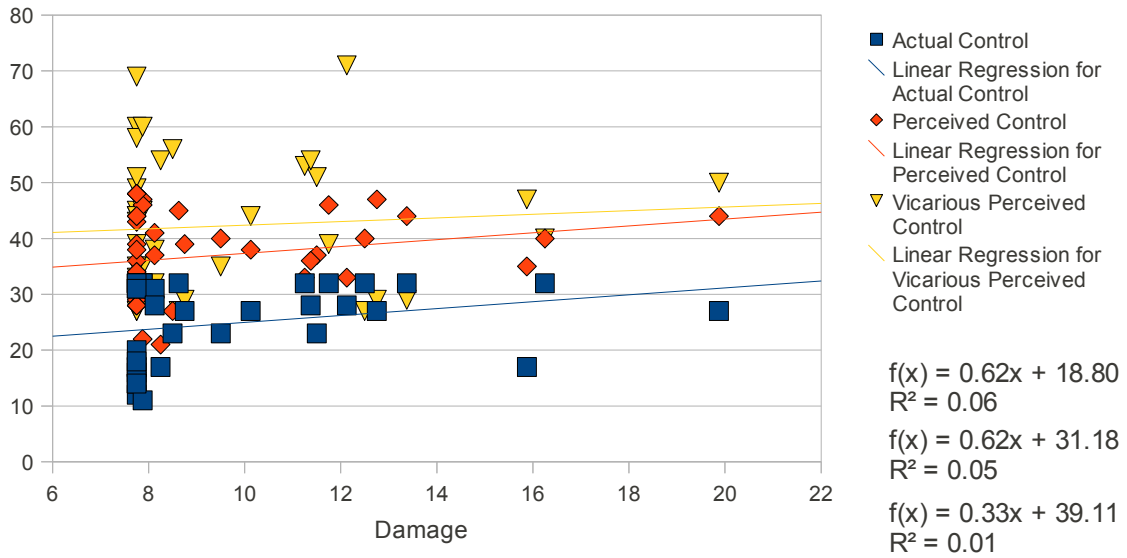

Illustration 4: Variables of Control vs Damage

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Unsurprisingly, as an organization's past experience with security incident-related damage increases, so does the individual's perception of the amount of control the organization exerts over them. Somewhat surprisingly though, as damage increases, so does the control that an individual has over their system. It was initially thought that this was due to the likelihood that the more responsibility an individual has for security, the greater knowledge they would have as to past incidents.

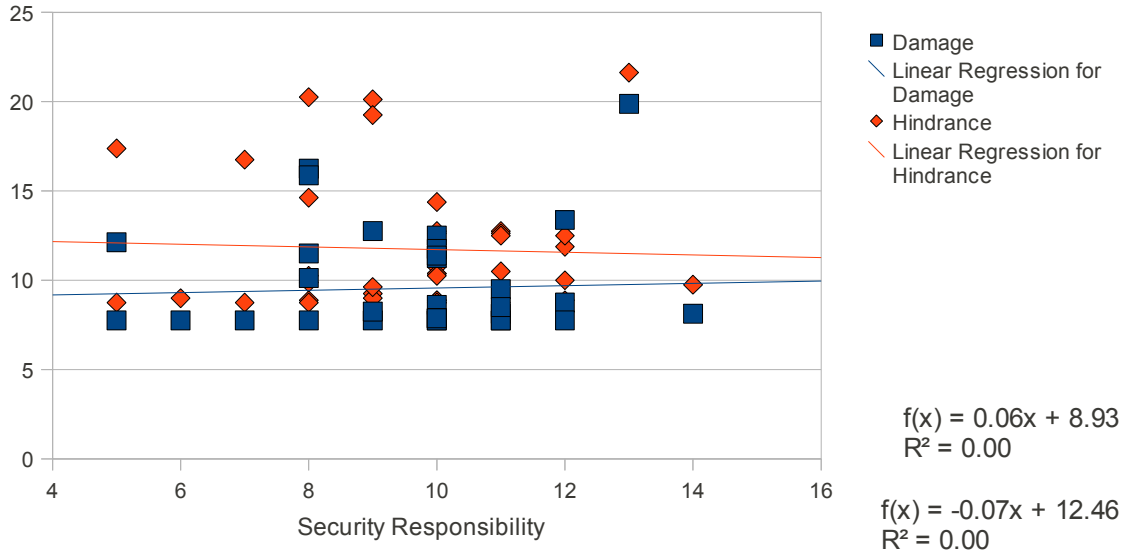

Illustration 5: Damage and Hindrance vs Security Responsibility

However, that does not seem to be the case. One's level of responsibility for security does not seem to have much impact on either the damage experienced from security incidents or on the amount of hindrance that security technologies cause.

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

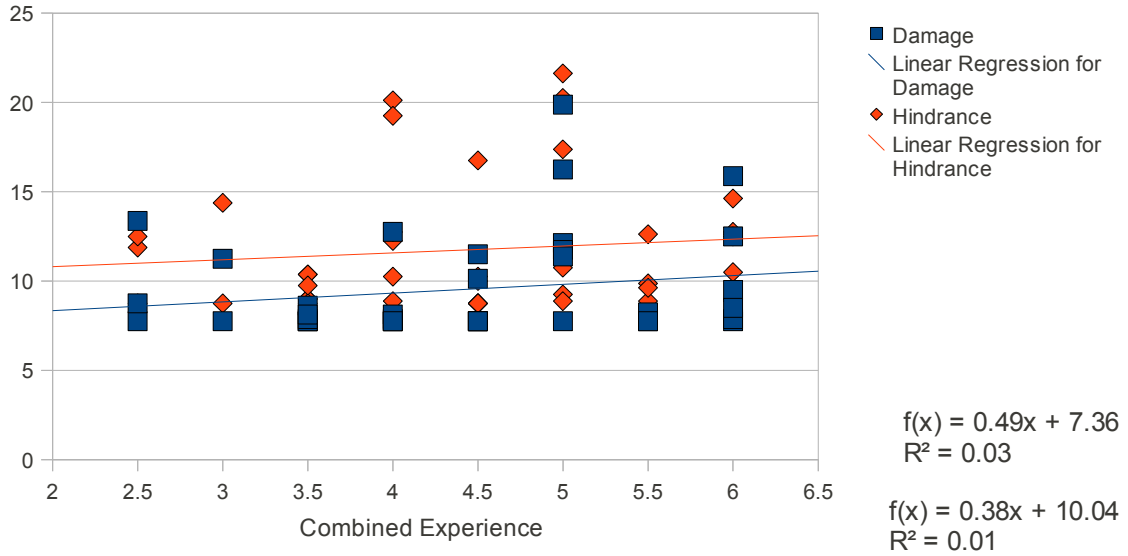

Illustration 6: Damage and Hindrance vs Combined Experience

It does appear that both damage and hindrance trend with one's experience in the workplace. However, since experience doesn't trend with control (Illustration 2), this does not explain the observation of damage trending with control.

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

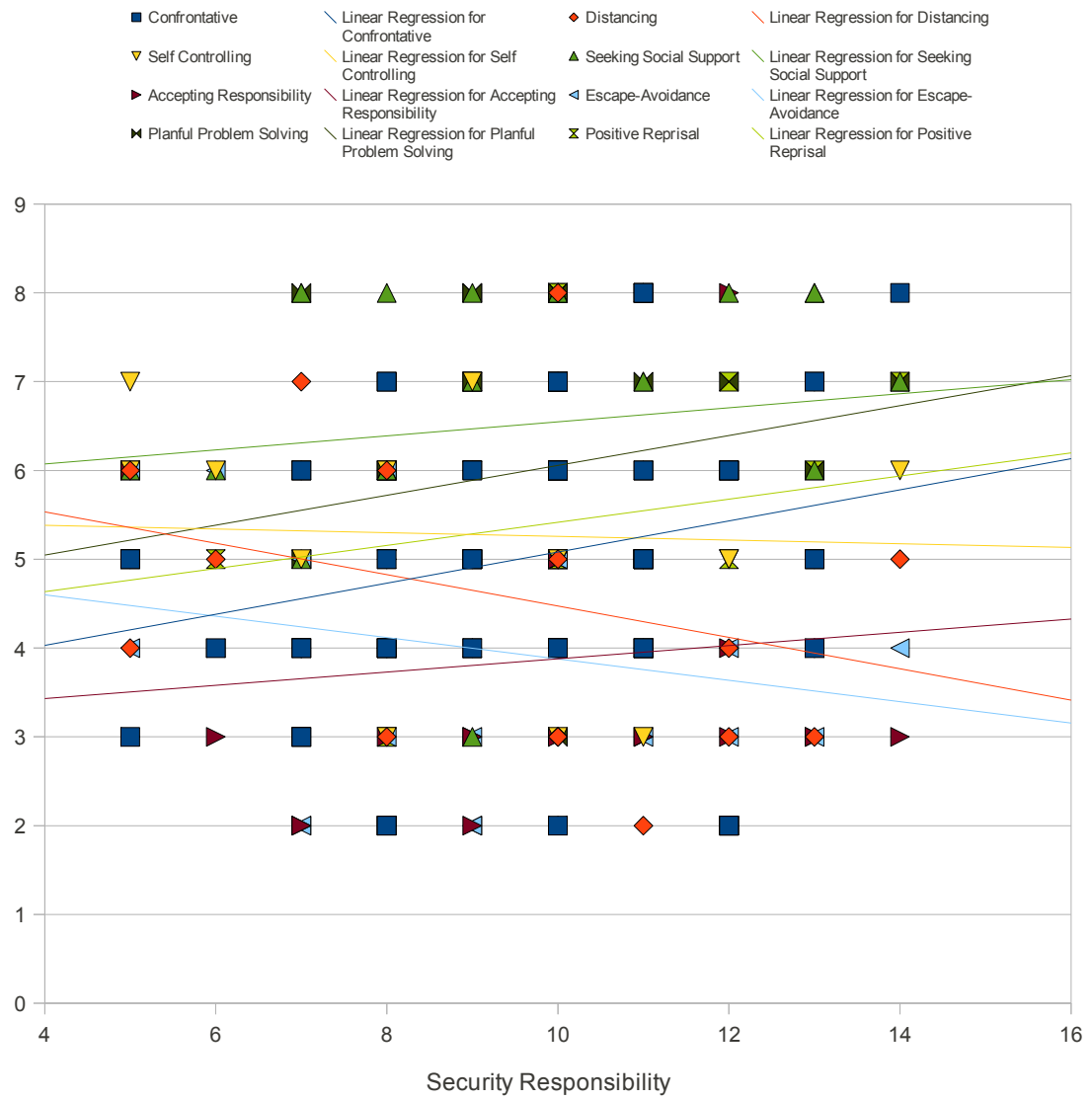

Illustration 7: Security Responsibility and Styles of Coping

Lastly, while there was insufficient data to fully analyze the styles of coping from the Personal Risk portion of the survey, preliminary trending estimates do show some interesting patterns. The higher a level of security responsibility that an individual has, the less they seem to engage in distancing and escape-avoidance and the more they engage in coping techniques such as confrontative, positive reprisal and planful problem solving with slight positive trending on accepting responsibility and seeking social support. It is unsurprising that successful security practitioners would exhibit these traits. However, whether security practitioners became successful because they already utilized these techniques or whether they developed these techniques in order to become successful is unknown.

Josh More, jmore@starmind.org

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Conclusions

In our experiment, the data appears to support the general assumptions around Actual Control, Perceived Control and Vicarious Perceived Control. The variables trend as expected when compared against the level of security responsibility held by the respondents. Individuals with a greater level of responsibility have a higher level of control over their workstations than those with lower levels of responsibility. In that respect, this study represents a good first step at measuring the variables of control within a typical business environment. However, the data does not show the expected trends with regards to some of the adjustment variables. Thus, these variables are not useful to better fit the trending lines to the data.

The trending lines do not fit the data as well as it would be preferred. While it will be very unlikely to get an R^2 close to unity with a widely ranging data set like this, higher values would be better. This would likely occur were the study done within a more unified environment, such as a group of similarly-sized companies.

The attempt to measure damage from user observation was unsuccessful. While some individuals shared some information as to losses, it did not seem correlate to anything. This could be due to lack of sufficient data, poor memories on the part of the respondents or that the respondents simply lacked the information to respond appropriately.

Also, some unexpected and interesting patterns emerged from the measurement of the personal sense of risk. These should be explored in greater depth in future studies, as they could help to proactively identify individuals that would thrive within a security-focused role. While the other variables measured could have an impact on how an organization deploys restrictive security technologies, these coping strategies could impact how an organization hires to staff a security team.

However, the fact some trends were noticeable lends support to the idea that a user/computer pair may be modeled as a biological entity. While it is clearly limited, due in part to the lack of consistency of users self-reporting how much damage past security incidents have caused, the correlation is close enough to indicate that the model has some value. The simple method explored here can be used to measure control variables across organizations. A larger number of respondents from specifically-targeted industries

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

would help to identify whether the variables correlate by industry type, business size or job role.

Fundamentally, there was sufficient trending in the data to indicate that the model works. The simplified statistical model functioned sufficiently well. More complex statistical analyses could be useful, but more data is required to really explore this area. One disadvantage of this model is that, like all models, it is only an approximation of reality. With further work and refinement, it can better fit every day situations, but it will never be a 100% match. This has to be taken into consideration as results are extrapolated. One advantage to using this model includes the ability to measure a user's psychology and help identify causes to security failures. Since individuals do not follow security policies in the same way that technology does, it is important not to ignore the "human factor" when reviewing incidents. This model provides one such method of measurement, and should be sufficiently simple to be used in many organizations.

Further Research

One challenge, of course, is that it is significantly easier to measure "how sick" a person is from a particular disease than it is measure "how hacked" a network may be. If monitoring technologies have not been deployed or if the network has been compromised by highly skilled attackers, the administrators may simply not have the data to estimate progression of compromise the same way that medical practitioners can estimate, for example, the stages of a cancer. More work needs to be done in this area to achieve better correlation to the work being done in the medical and psychological sciences.

Of all of the variables discussed in this paper, an important one that's missing is the difference between vicarious actual control and vicarious perceived control, as it could predict the amount and severity of risks that users will take. Doing such a study, however, would entail measuring "both sides of the equation" so to speak, and having those in charge of technical restrictions answer a separate questionnaire. This would gather information about user perceptions and technical controls, so they could be compared. This would be an excellent avenue for future research.

It is worth noting that some psychologists prefer to separate perceived control into two variables: Locus of Perceived Control (LPC) and Focus of Perceived Control (FPC),

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

where LPC measures how perceived control can impact a condition and FPC measures how perceived control can alleviate symptoms of a condition (Beckjord, Glinder, Langrock, & Compas, 2009). However, as significantly more work has been done to objectively measure the progress of a disease than the gradual worsening of the security of an environment, it would be impractical to attempt to draw this distinction at this stage of the research. As the field of information security matures, finer grained measurement of these issues may become more feasible.

There is also evidence that going through focused disease-management training is beneficial to quality of life, for manageable diseases (Olajos-Clow, Costello, & Lougheed, 2005). Disease management programs seem to be more focused on specifics than many security training programs. And in the asthma study in particular, a surprising number of individuals did not complete the program (Olajos-Clow, Costello, & Lougheed, 2005) . However, as studies seem to indicate that training creates an increased sense of control and that an increased sense of control minimizes symptoms, more attention should be focused on security training with an emphasis on changing behavior, not as a compliance check item or knowledge transfer alone, but as a way to ensure the smooth operation of the business.

As one attempts to change behavior, though, one must be aware of the problems forecasted by Learned Helplessness Theory. Though beyond the scope of this paper, this theory suggests that in some ways, usually when faced with negative reinforcement, people learn to be helpless. Thus, even when control is given back to them, some people will persist in their prior helpless behavior. Thus, if an organization wishes to improve their security posture by empowering their employees, they must work to overcome this tendency. For more details, see the work of Burger and Arkin (Burger & Arkin, 1980), as well as introductory psychological texts.

These non-measured multi-dimensional aspects of perceived control may involve how the variable impacts overall risk, severity of threat, and the speed and efficacy of threat response or leveraging existing defensive technologies.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

References

Adams, J. (1996). *Risk.* London, UK: Routledge.

Beckjord, E.B., Glinder, J., Langrock, A., & Compas, B.E. (2009). Measuring multiple dimensions of perceived control in women with newly diagnosed breast cancer. *Psychology and Health, 24*(4), 423–438.

Burger, J.M., & Arkin, R.M. (1980). Prediction, control, and learned helplessness. *Journal of Personality and Social Psychology, 38*(3), 482-491.

Du, S., Keil, M., Mathiassen, L., Shen, Y., & Tiwana, A. (2006). The role of perceived control, attention-shaping, and expertise in it project risk assessment. *Proceedings of the 39th Hawaii International Conference on System Sciences*

Eklund, M., & Backstrom, M. (2006). The role of perceived control for the perception of health by patients with persistent mental illness. *Scandinavian Journal of Occupational Therapy, 13*, 249-256.

Folkman, S., Lazarus, R.S., Dunkel-Schetter, C., DeLongis, A., & Gruen, R. (1986). Ways of coping checklist, revised 1985. Retrieved from http://www.caps.ucsf.edu/tools/surveys/pdf/Ways%20of%20coping.pdf

Helgeson, V.S. (1992). Moderators of the relation between perceived control and adjustment to chronic illness. *Journal of Personality and Social Psychology*, *63*(4), 656-666.

Helgeson, V., & Franzen, F. (1997). The role of perceived control in adjustment to diabetes. *Anxiety, Stress and Coping, 11*, 113-136.

Hopfield, J.J. (1982). Neural networks and physical systems with emergent collective computational abilities. *Proc. NatL Acad. Sci. USA*, *79*, 2554-2558.

Kasunic, M. (2005). Designing an effective survey. Handbook, Software Engineering Institute, Carnegie Mellon, Pittsburgh, PA. Retrieved from http://www.sei.cmu.edu/reports/05hb004.pdf

Olajos-Clow, J., Costello,, E., & Lougheed,, M.D. (2005). Perceived control and quality of life in asthma: impact of asthma education. *Journal of Asthma, 42*, 751–756.

Rand, Initials. (n.d.). Rand 36-item health survey 1.0 questionnaire items. Retrieved from http://www.rand.org/health/surveys_tools/mos/mos_core_36item_survey_print.html

Ruthig, J.C., Perry, R.P., Hladkyj, S., Hall, N.C., & Pekrun, R. (2008). Perceived control

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

and emotions: interactive effects on performance in achievement settings. *Soc Psychol Educ*, *11*(2), 161-180.

Schneier, B. (2008, October). Does risk management make sense? [Web log message]. Retrieved from http://www.schneier.com/essay-240.html

Taylor, S.E., & Brown, J.D. (1988). Illusion and well-being: a social psychological perspective on mental health. *Psychological Bulletin, 103*(2), 193-210.

Wallston, K.A., Wallston, B.S., Smith, S., & Dobbins, C.J. (1987). *Perceived control and health. Current Psychological Research and Reviews, 6*(1), 5-25.

Weinstein, F., Healy, C., & Ender, P. (2002). Career choice anxiety, coping, and perceived control. *The Career Development Quarterly*, 50, 339-349.

Josh More, jmore@starmind.org

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced