Future directions for behavioural information security research

Jayesh Surana(Assistant Professor), Aditi Sharma, Barkha Bulani, Chinu Mangal, Ishan Neema

Information Technology, Shri Vaishnav Instiitute of Technology and Science, Gram Baroli, Indore, Madhya Pradesh, India

Abstract:

In an organization it is seen that some employees who seem to be a weak link in Information Security can sometimes prove to be a big asset in making a great effort to reduce all the risks related to Information Security. The employees who abide by the rules and regulations related to Information Security are the ones who basically lead to strengthening Information Security and understand that such a behaviour is the necessity and crucial to the company's capital. Information Security (Infosec) includes ways to protect and mitigate any kind of threats that may occur in any system. The main aim of this paper is to concentrate on the Future Directions for Behavioural Information Security research. It mainly highlights the currently faced problems and also future directions regarding the field of information security needs to be explored.

1. Introduction:

Information Security research deals with many different aspects and fields like: Philosophical, Behavioural, Technical, Managerial and many more. It has also even dealt with fields like socio philosophical and socio organizational, it has mainly dealt with prevention and detection of intrusions and several different kinds of attacks. These are important aspects and needs to be dealt with carefully but one thing that is not looked upon or lacked behind regarding security matters is the individuals in an organization. It's been seen and estimated that more than half f the intrusions or the attacks that take place are because of the insiders that reside and work in the particular organization.

Behavioural Information security is a part or a branch or a classification of broad category information security that includes or look upon the behaviours of the individuals that work in an organization for protecting information and assets. Several studies have been conducted and several theories have been applied to see the actual performance of individuals regarding protection and security. Inspite of these studies and theories there are still some challenges that are faced and needs to be taken care of. This paper aims to address them and also the results from such analysis that needs to be explored.

2. Future behavioural research directions:

The research is based on several different categories as follows:

- Intentions of individuals in an organization
- Facts about the hackers
- Ways to improve Infosec compliance
- Advance Infosec research

2.1.1. Intentions of individuals in an organization

A significant effort has been seen to investigate human perpetrators of IS security threat, especially from those who are within the organization. Based on their intentions these sources of threat were further characterized. The focus been on IS security policy non-compliance by employees, i.e., within the behavioral research community. Such acts may be:

- intention-based, willful, malicious violation (such as sabotage, data theft, data destruction, etc.) or
- they may be unintentional or accidental actions, including forgetting to change passwords, failing to log off before leaving a workstation, or careless discarding of sensitive information rather than shredding it.

Warkentin (1995) expanded the taxonomy to include low-grade and high-grade threats; the latter being a purposeful individual or organization who will seek obscure vulnerabilities and inflict far greater economic damage by maintaining intrusions for the maximum long-term gain. So we can say that risks from intentional human activity are highly dangerous, especially with sophisticated hackers, spies, terrorists, and criminal organizations that are committed to coordinate global attacks on secret information assets in order to achieve their goals in a wide range and massive destruction. Some malicious attackers wish to damage and inflict loss for political reasons or for military purposes, identity theft, and other criminal acts.

New classes of increasingly devious and effective malware capable of penetrating even the most recent perimeter defenses have posed more risks. These include viruses, Trojan horse, worms and distributed BotNet attacks. But the greatest threat as of till date is the attack from the inside - the organizational member who is a trusted inside the firewall to perform different tasks. This employee with a valid username and password regularly access the information assets of the organization. Employees can pose great harm to the confidentiality, integrity, or availability of the IS through deliberate activities (disgruntled employee or espionage) or they may introduce risk via laziness, sloppiness, poor training, or lack of motivation to vigorously protect the integrity. The insider threat has repeatedly been called the greatest threat to information security, and yet this is often overlooked in a rush.

2.1.2 Facts about the hackers

Cyber security is becoming an important concern for individuals and organizations with the widespread use of computer and internet. Risks of data breaches via malicious software are faced by many organizations now days henceforth compromising their business. One major risk still not studied properly by the IS scholars is the mysterious world of computer hackers. With the various definitions of hackers that exist, has made their study even more difficult. At a high level, hackers refer to those people who attack an organization's information systems infrastructure for a variety of reasons, and can be viewed as state hackers, terrorists, non-state hackers/organized crime, disgruntled employees/insider attackers, hobbyists, script kiddies and legitimate penetration testers. The definition of hackers and crackers have always been confused, crackers are those people who hack into systems to damage people or companies via the Internet. However, in the 1980s law enforcement began to use the term hackers for people who met this definition.

The first challenge in researching the hacker community is accurately defining the group of people that are being investigated. Each type of hacker will have their own reasons why they perform the behaviors they do, making proper definition of the context crucially important. The evolutionary stages that young hackers go through of starting with "hacking for fun," progressing to a "do no harm" starting with "hacking for fun," progressing to a "do no harm" approach and finally resulting in hacking for survival or for profit. An avenue for future research would be to expand on this approach and provide more differentiation on the behavioral motivations of these different types of hackers.

The primary challenge in hacking research is gaining access, regardless of the type of hacker being studied. Hackers are not easily identifiable and hacking activities are conducted in secret. Hackers and hacking activities are unpredictable. That is their modus operandi, their motive and the time when they might strike. A sophisticated group of scholars have been studying their traces and modus operandi for decades but they just get different by every attack. Hacker assets come in different forms. Three of the most commonly used assets are attachments, source code, and tutorials.

2.1.3 Ways to improve Infosec compliance

The disparate nature of the influence of fear on individual security outcomes underscores the difficulty in conducting research in this area, but also offers a hope of opportunity for a meaningful contribution to knowledge.

The connotation of the word 'fear' has further complicated the study of fear-based persuasive messages. Fear is as powerful of a motivator as it is in the context of the extant research from which this construct has been adapted. The magnitude of fear is different for someone being diagnosed with cancer and different for someone experiences when faced with threats to data or computer systems. The emotion experienced in these two settings may be completely different and have different characteristics. Rate of dissipation, potential to interact with other factors, unique manifestation and intensity in individuals, relationship to coping appraisal, and how it is translated into behavior can be such characteristics. Fear is likely a multi-faceted construct that can manifest itself in different degrees that are highly relevant to Behavioral InfoSec research.

Behavioral InfoSec research that captures perceptions of fear does so via a survey methodology or embedded within a lab experiment. It raises another confound in whether a clearly artificial laboratory setting can accurately represent the fear that users experience in the moment their information is compromised or when they are caught violating information security policies both situations obviously cause higher levels of fear than in a hypothetical scenario situation presented in the laboratory. The level of fear can’t be matched with the laboratory and in the real life. The ear in real life is highly amplified at times which is difficult to present in laboratory terms.

Another area of research would investigate the dynamics of fear over time, as users react to events they encounter when interacting with technologies that may pose perceived threats. The investigations on the real time dynamic fear appeal are based on their current actions. The real time fears the same fear that we talked above about real life. As the magnitude and level of fear can’t be judged just by the laboratory.

2.1.4 Advance Infosec Research

One of the biggest issues and limitations of Behavioral InfoSec research is that the majority of it has been conducted in Western cultures, with occasional studies being conducted in Asia and elsewhere

Classifying or measuring national culture is a great challenge, because it is an entity comprised of various aspects of individual behaviour. In this study we use Hofstede’s cultural dimensions to understand how an intercultural approach can be used to improve InfoSec training and compliance with InfoSec best practices. Here Hofstede model is been choosen because it encompasses over 30 years of experience and has been used worldwide in cross-cultural training programmes. In past,the cultural dimensions for InfoSec was only implicitly addressed. The uncertainty avoidance index (UAI) as the extent to which members of a culture feel threatened by uncertain or unknown situations. Denmark and Singapore are examples of low uncertainty-avoidance national cultures; whereas Japan is an example of high uncertainty avoidance. According to InfoSec context, it suggests that Japanese end-users will be less likely to fall prey to phishing emails due to their uncertainty. Conversely, Singaporean users are less likely to by the uncertainty involved in phishing solicitations.

Another dimension of national culture is individualism (IDV) or the loose ties between individuals compared to more collectivistic countries where people are integrated into strong, cohesive groups that protect individuals in exchange for unquestioning loyalty. The United States is an example of high individualism in contrast to China that is highly collectivistic. These differences could have an impact on users’ InfoSec behaviours. Stronger loyalty in collectivistic individuals may lead to stronger adherence to InfoSec policies. However, a negative aspect is that the same person might be less likely to report InfoSec violations of people to whom they are loyal. In individualistic cultures, employees should be more likely to whistle-blow substantial InfoSec violations regardless of existing loyalty and relationships.

In the extent of Power Distance (PDI) members of institutions and organizations within a country who are less powerful, expect and accept that power is unequally distributed. Thus, high power distance cultures like China, are more likely to comply with new policy requirements, while those in low power distance cultures such as Canada, may be more likely to question new InfoSec policies.

Another dimension of national culture is long- and short-term orientation (LTO) as perceived by Confucian dynamism. This kind of differences may have a significant impact on how leaders in organizations strategically plan their InfoSec architecture. It would be expected that InfoSec managers with a longer view such as Chinese and Japanese, would engage in more advanced, long-term planning that would focus on a scalable, highly secure architecture and policies for improving InfoSec. Those with a short-term view such as Americans or Canadians, might have a less broad vision and be more narrowly-oriented towards short-term goals.

National cultures can be also differentiated by a dichotomy of masculinity vs. femininity (MAS). By the feminine culture, human relationship values and concern for others has increased. On the other hand, masculine cultures are more assertive and value materialism. We can expect that individuals in masculine cultures such as the US, would be more likely to disobey the InfoSec policies in order to achieve success and demonstrate their superiority, while individuals in feminine cultures such as Denmark, would be more concerned about the consequences of their actions and thus would be less likely to break the rules.

2.2 Methodological challenges

One of the common themes in the discussion above is the need for better ways to collect and measure security related data.

2.2.1 Solution for methodological challenges

There should be some methodologies that provides solution for the methodological challenges. Therefore there are basically three methodologies that offers solution. They are: longitudinal studies, qualitative methodologies, controlled laboratory and field experiment methodologies.

The methodologies that are still rare and need to be fostered and encouraged is longitudinal and laboratory studies. It will be very useful to enrich the field of Behavioral InfoSec research, strengthening the theories and methodologies. It's use would help scholars to collect actual behavioral data effectively that are not possible to collect in snapshot survey research. Since actual behavioral data is much more accurate and reliable than self - reported behavioral or behavioral intention data. So to investigate the explanatory power of theories on actual behaviors over an extended period of time utilizing longitudinal studies researchers by researchers would be a better option.

Methodologies following well-established scientific approaches are qualitative methodologies. It includes positivist and interpretive case studies and grounded theory that have started to emerge. To better understand the actual motivations and behaviors of the insiders it could provide an effective method.

To find out the difference between the actual and intentional behaviors of people there is an another approach i.e. controlled laboratory and field experiment methodologies. It is helpful in collecting more realistic behavioral data that can address the shortcomings of survey based research.

One consistent challenge for Behavioral InfoSec research is gaining access to individuals' actual behavior. Approach to address this challenge is to spoof real websites so that the actual user behavior is measured. Since it would involve deception, thus to assure the ethical treatment of the human subjects, extra care will be required. As new approaches address ethical concerns about collecting actual behavior data and also result in interesting findings regarding new data collection approaches therefore exploring unique new approaches to obtain data on actual behavior should not be prohibited.

Other research issues is why people engage in unethical behaviors. It is important to identify and use the appropriate research methodologies to find out the reason why people that are not generally willing to admit to committing these sorts of behaviors commit them. In order to collect behavioral data scenarios, incentives, and experiments are all used. Scenarios are finding use and provide an opportunity to capture anti-social and unethical behavior by presenting respondents with hypothetical information and ask them what they would do in that situation. This approach allows subjects to remove their own feeling of incrimination from their responses.

There is involvement of a certain agreement for how to capture data about deception and fraud mainly phishing attacks. There are many other information systems theories are also available that can help provide insight into how to make such a determination. One Information Manipulation Theory (IMT) is one such theory, which informs us that in deceptive message there are different types of deception used. These are manipulations of relevance, quality, clarity, quantity. As individuals are not very adept at detecting deception therefore the receiver will be deceived simply by manipulating messages in these different ways.

Suppose a researcher designed software artifacts that use IMT as a framework for detecting whether a potential insider is prone to future information abuse. Firstly, it's necessary to find characteristics of known insider abusers. It can be accomplished through data mining non-security related data. Uncovered information then can be used to help uncover other individuals that may have potential to become insider threat.

These methodologies and solutions to the challenges of data collection will help to improve the validity of future research. In order to develop practical security solutions to the problems facing enterprise managers it will provide practitioners with a more solid foundation. It will also help in thoroughly finding the insider behavior which will be a great asset for enterprises to save there data and enforce strict security measures.

3. Conclusion

There are so many issues at the intersection of people, technology, and organizations, thus in order to explore such issues many opportunities are provided by Behavioral InfoSec.

Finding difference between intentional and unintentional behavior, focusing attention on developing ways to measure security related behaviors, data collection from websites and spoofing them, etc will be a very fruitful avenue for future research. By properly measuring actual behaviors many of the issues are identified in this research paper. There are many methodologies and tools that will help in addressing problems and help in overcoming them even though they are not easy to implement. There should also be exploration and discoveries of new approaches and technologies beyond the traditional ones.

Tackling the challenges and finding suitable solutions will have practical ramifications that extend beyond just the interests of the research community. Firstly, the steps can be taken to improve their positive security behaviors while decreasing their negative security behaviors by understanding security behaviors of individuals. Further, it may also provide insight into the implementation and design of security subsystems. The design of new technology artifacts will lead to development of a new piece of technology. Opportunities for creating or enhancing new information security tools will arise when new factors relating to individuals securing their information assets come to light.

References:

Ajzen I. Attitudes, personality and behavior. New York, NY: Open Univ Press; 2005.

Barber R. Hackers profiled e who are they and what are their motivations? Computer Fraud & Security 2001;2001(2):14e7.

Choo K-KR. The cyber threat landscape: challenges and future research directions. Computers & Security 2011;30(8):719e31.

D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate Glaser BG, Strauss AL. The discovery of grounded theory: strategies of qualitative research. London: Wledenfeld and Nicholson; 1967.

s.amazonaws.com/academia.edu.documents.Information_security_policy_compliance

Behavioral_and_policy_issues_in_information_systems_security_The_indider_threat