Health IT Security Journal

Volume 2, No. 3

A publication of the HITSF

Health IT Security Journal

Volume 2, No. 3

HITSF

IN THIS ISSUE

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Editor in chief: Hadi Syahrial

Review Board

- Eric Vanderburg
- Dr. Nurhizam Safie
- Dr. Moedjiono
- Dr. Lukas

Editorial Board

- Bambang Suhartono
- Gregorius Bimantoro
- Seyed Mohammad Motahar

Letter from the editor

Dear readers,

This is the second year of the Journal and we are proud to present another issue. This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

www.healthitsecurity.org

Criteria for Selecting a Risk Assessment Methodology

by Eric Vanderburg

Risk assessment is the process of identifying vulnerabilities, threats, and risks associated with organizational assets and the controls that can mitigate these threats. Risk managers and organizational decision makers use risk assessments to determine which risks to mitigate using controls and which to accept or transfer. There are two prevailing methodologies for performing a risk assessment. These are the qualitative and quantitative approaches. A third approach, termed mixed or hybrid, combines elements of the qualitative and quantitative approaches.

Quantitative

Quantitative risk assessments use mathematical formulas to determine the exposure factor and single loss expectancy or each threat as well as the probability of a threat being realized called the Annualized Rate of Occurrence (ARO). These numbers are used to estimate the amount of money that would be lost to exploited vulnerabilities annually called the Annualized Loss Expectancy (ALE).

With these numbers the organization can then plan to control this risk if countermeasures are available and cost effective. These numbers allow for a very straightforward analysis of the costs and benefits for each countermeasure and threat to an asset. Countermeasures that reduce the annualized loss expectancy greater than their annualized cost should be implemented if there is sufficient resource slack available to employ the countermeasure.

For example, a quantitative assessment for Company X identifies $1,000,000 in assets and due an exposure factor of 1%. Company X expects to lose $10,000 annually. In other words, the ALE is $10,000. Countermeasures are available that will reduce this expectation to $2,000 per year and the countermeasures cost $7,000 per year to implement. This assessment makes it easy to see the savings of implementing the countermeasures because the organization would save $1,000. The math is as follows: $10,000 loss reduced to $2,000 is a reduction of $8,000. The countermeasures cost $7,000. $8,000 reduction in loss minus $7,000 for the cost of the countermeasures equals a savings of $1,000.

SIDE NOTE:

Single Loss Expectancy (SLE) SLE=Asset Value * Exposure Factor

Annualized Loss Expectancy (ALE) ALE=SLE* Annualized Rate of Occurrence (ARO)

As you can see, the formulas here are all based on the asset value and exposure factor. Therefore, different quantitative risk assessments could produce very different results if the method of asset valuation differed. One assessment may use purchase cost as the asset value but another may use value to data owners, operational cost, value to competitors, or the liability associated with asset loss. Each of these values would be reasonable to use but they would produce different results.

In the example above, the decision to implement the countermeasures would be different if the asset valuation turned out to be $850,000 instead of $1,000,000. Here the ALE would be $8,500. Now the loss if still reduced to $2,000 would result in a savings of $6,500 but the countermeasures cost $7,000 so the organization would lose $500 implementing the countermeasures. It is important to recognize how different methods of asset valuation impact the assessment. The methods used in asset valuation should be documented so that decision makers understand how the numbers were obtained.

Qualitative

Qualitative risk assessments use experience, judgment, and intuition rather than mathematical formulas. A qualitative risk assessment may utilize surveys or questionnaires, interviews, and group sessions to determine the threat level and annualized loss expectancy. This type of risk assessment is very useful when it is too difficult to assign a dollar value to a specific risk. This can easily be the case with highly integrated systems that house numerous assets and are subject to a variety of risks.

Qualitative assessments are usually well received because they involve many people at different levels of the organization. Those involved with a qualitative risk assessment can feel a sense of ownership of the process. Qualitative risk assessments do not require a great deal of mathematical computation but the results are usually less precise than those achieved with a quantitative assessment.

Mixed

It is possible to use a mixed approach to risk assessments. This approach combines some elements of both the quantitative and qualitative assessments. Sometimes quantitative data is

used as one input among many to assess the value of assets and loss expectancy. This approach gives the assessment more credibility due to the hard facts presented but it also involves people within the organization to gain their individual insight. The disadvantage of this approach is that it may take longer to complete. However, a mixed approach can result in better data than what the two methods can yield alone.

Summary

Risk assessments can use a quantitative or qualitative methodology or a combination of the two to determine asset valuation, threat levels, and the annualized loss expectancy due to vulnerabilities. There are software applications that will make performing quantitative calculations easier for risk assessments so this approach is quite useful for those new to risk assessment. Quantitative assessments provide clear data that makes decision making easy. However, qualitative assessments utilize experience and may uncover things missed by a pure mathematical formula. Qualitative assessments also involve more people which can aid in the acceptance of results.

About the Author:
Eric Vanderburg

Director, Information Systems and Security, JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

User Security Behaviours

by Hadi Syahrial

One of the most dangerous security threats today is internal threat. The Internal Security Threat is a threat area encompassing a broad range of events, incidents and attacks all connected by being caused not by external people who have no right to be using the corporate IT facilities but by the company's own staff, its authorised IT users [1].

To manage down the internal security threat, we need to understand how a company's culture and practices can affect people's behaviour [1].

According to John Leach [1] the influential factors fall into two groups, as illustrated in the diagram below. The first group, encompassing the user's understanding of what behaviours the company expects of them, is distinct from the second group, factors which influence the user's personal willingness to constrain their behaviour to stay within accepted and approved norms.

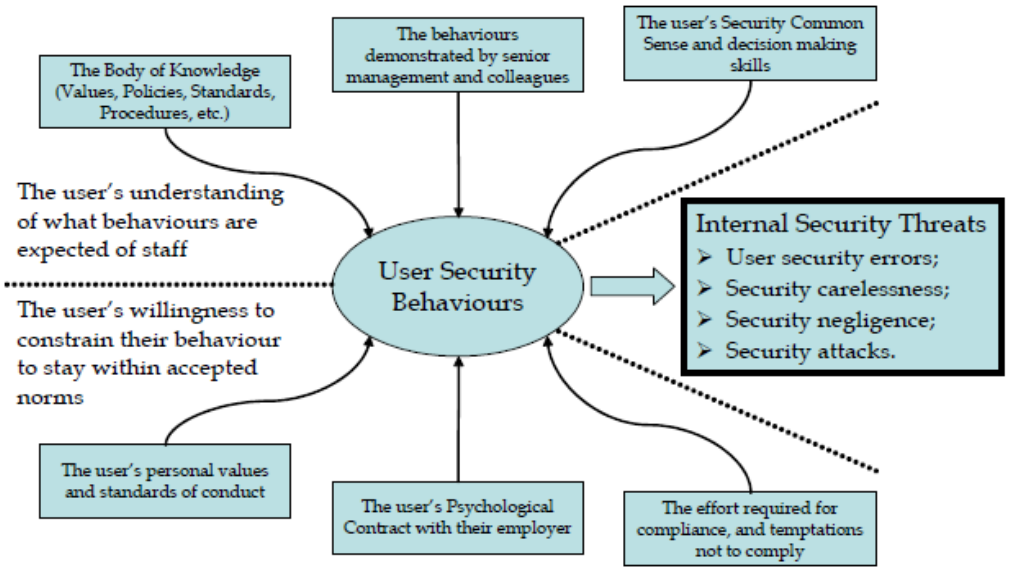


Figure 1: The Factors That Influence User Security Behaviours

The user's understandings of which behaviours are expected of them – shown in the top half of the diagram - are formed from:

- What they are told;
- What they see being practiced by others around them;
- Their experience built from decisions they have made in the past.

Security behaviour can also be described using a two-factor taxonomy, where the two factors are intentionality and technical expertise [5]. As shown in Figure 2, this creates six categories of security behaviours, where two of those behaviours (Aware Assurance and Basic Hygiene) are positive, designed to increase security, and four of the behaviours may result in breaches to security.

Figure 2: Two-factor taxonomy of end user security behaviours [5]

In fact the majority of human factor errors could be described as accidental. Accidental human factor errors are associated with the way in which the individual interacts with a system, and evidence suggests that people may encounter problems in finding, understanding and using security features [6].

Some evidence suggests that employees' failure to comply with information security guidelines is the cause of the majority of breaches in information security [2]. One common human error that can lead to security breaches is referred to as a capture error. Such errors occur when a familiar activity or habitual routine takes over (or captures) an unfamiliar activity, leading to a cognitive failure or mistake [3]. These errors are particularly common during periods of tiredness or inattention.

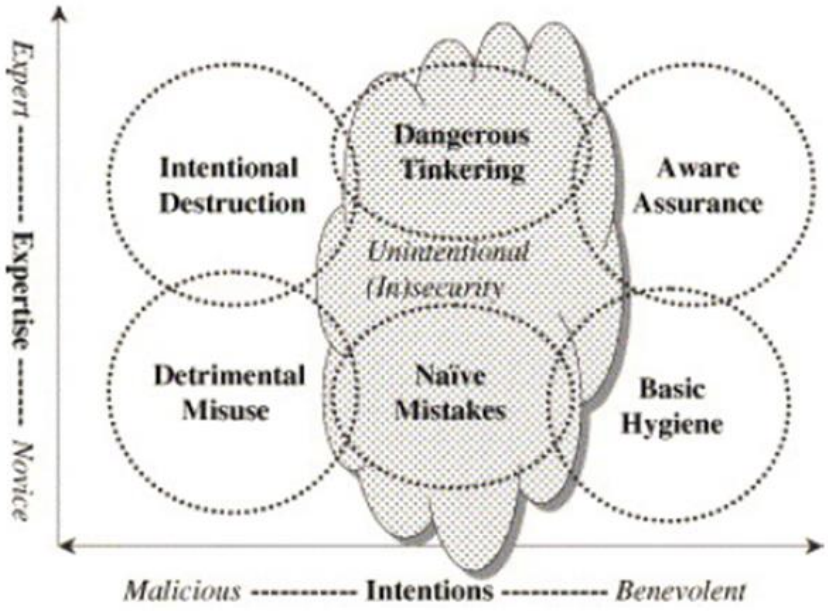
There are five different types of human factor errors, which can be used to explain information security breaches. First, there are acts of omission, in which people forget to perform a necessary action. For instance, in an information security domain, this could involve the failure to regularly change passwords. Second, errors are commonly acts of commission, in which people perform an incorrect procedure or action, such as writing down a password. Third, a number of errors are caused by

extraneous acts, which involves doing something unnecessary. Fourth, errors can be caused by sequential acts, which involve doing something in the wrong order. Fifth refer to time errors, caused by people failing to perform a task within the required time [4].

Inattention and tiredness can also result in post-completion errors, in which the individual neglects to carry out a necessary 'tidy-up' or 'clean-up' action that is required after the main goal has been completed [7]. For example, from an information security point of view, the main goal may involve sending an email from a secure system. Once that goal has been completed, it is then necessary to complete the final action of logging off the system. A post-completion error would involve a situation where the individual in question fails to complete that final task, leaving the system open to a possible security breach.

Since 2001, the CERT Insider Threat Center has conducted a variety of research projects on insider threat. One of our conclusions is that insider attacks have occurred across all organizational sectors, often causing significant damage to the affected organizations. Examples of these acts include the following:

- low-tech attacks, such as modifying or stealing confidential or sensitive information for personal gain
- theft of trade secrets or customer information to be used for business advantage or to give to a foreign government or organization
- technically sophisticated crimes that sabotage the organization's data, systems, or network



In many of these crimes, damages extend beyond immediate financial losses. Widespread public reporting of the event can severely damage the victim organization's reputation, over both the short and long term. A damaged reputation almost invariably leads to financial losses [8].

Summary

End-user security behaviours are an important part of enterprise-wide information security. Security failures could be the result not of poor security solutions but of poor security behaviour by staff.

References:

[1] John Leach (2003). Improving User Security Behaviour, John Leach Information Security Limited.

[2] Chan, M., Woon, I. & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior, Journal of Information Privacy and Security, 1(3), 18-42.

[3] Norman, D. A. (1981). Categorization of action slips. Psychological Review, 88(1), 1-15.

[4] Swain, A. D., & Guttman, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278, U.S. Nuclear Regulatory Commission, (Washington D.C.).

[5] Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviours. Computers and Security, 24, 124-133.

[6] Furnell, S. (2005). Why users cannot use security. Computers and Security, 24, 274-279.

[7] Anderson, R.J. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). New York: Wiley.
[8] TECHNICAL REPORT CMU/SEI-2012-TR-012, Common Sense Guide to Mitigating Insider Threats
4th Edition, 2012.

About the Author:

Hadi Syahrial

Hadi Syahrial is a Lecturer and Researcher at Budi Luhur University, Jakarta, Indonesia.