Assessing Security Protection for Sensitive Data

George O.M. Yee
Aptusinnova Inc. and Carleton University
Ottawa, Canada
email: george@aptusinnova.com, gmyee@sce.carleton.ca

***Abstract*—The growth of the Internet has unfortunately been accompanied by an increasing number of attacks against an organization's computing infrastructure, leading to the theft of sensitive data. In response to such incursions, the organization installs security measures (e.g., intrusion detection system) for protecting its sensitive data. However, this installation is often done haphazardly, without any objective guidance regarding how many vulnerabilities must be secured in order to achieve a targeted level of protection that would be deemed acceptable. This work derives estimates of the levels of protection based on the number of vulnerabilities to attack that have been secured. The paper then shows how an organization can calculate these estimates, and use them to adjust the number of security measures installed, until a certain target level of protection is achieved subject to certain constraints. An application example is included.**

Keywords-assessment; security; protection; sensitive data; vulnerability.

I. INTRODUCTION

Recent attacks against computing infrastructure, resulting in the theft of sensitive data, have grabbed the headlines, and have devastated the victim organizations. The losses have not only been financial (e.g., theft of credit card information), but more importantly the damage to the organization's reputation. Consider the following data breaches that happened in 2016 [1]:

- February, 2016, University of Central Florida: Data breach affected approximately 63,000 current and former students, faculty, and staff, with the theft of information including social security numbers, first and last names, and student/employee ID numbers.
- February, 2016, U.S. Department of Justice: Hackers released data on 10,000 Department of Homeland Security employees one day, and the next day released data on 20,000 FBI employees. Stolen information included names, titles, phone numbers, and email addresses.
- March, 2016, Premier Healthcare: Theft of a laptop containing sensitive data pertaining to more than 200,000 patients, including names, dates of birth, and possibly social security numbers or financial information.
- March, 2016, Verizon Enterprise Solutions: Hackers stole information for about 1.5 million customers; the information was found for sale in an underground cybercrime forum by cyber security journalist Brain Krebs.
- September, 2016, Yahoo!: The company announced that a hacker had stolen information from 500 million accounts in 2014. The hacker, believed to be working for a foreign government, stole email addresses, passwords, full user names, dates of birth, telephone numbers, and in some cases, security questions and answers.

This is only a sampling, as there were many more breaches in 2016, and in fact, no year can be said to have been breach-free.

To protect themselves from attacks, such as the ones described above, organizations determine their vulnerabilities to attack, and then secure the vulnerabilities with security measures. Common measures include firewalls, intrusion detection systems, two-factor authentication, encryption, and training for employees on identifying and resisting social engineering. However, today's organizations install security measures without any way of calculating the overall level of protection that will result. They proceed based on recommendations from consultants or in reaction to attacks that have been observed. And in many cases, they are forced to stop this deployment once their security budget runs out. It would be far better if an organization can follow a top-down approach, by setting a target level of protection and then install security measures to achieve the target. The target would be set according to the expected threat situation, the nature of the business, the sensitivity of information kept, and an estimated financial budget. Before this can be done, it would be useful to have quantitative estimates of the level of protection based on the number of vulnerabilities secured. This work derives such estimates and shows how to apply them to not only set a protection target, but also how security measures can be installed to achieve the target.

The objectives of this work are i) derive estimates of the resultant protection level obtained by an organization through the installation of security measures to secure vulnerabilities, ii) show how these estimates can be calculated, iii) show how the estimates can be applied in a top-down and objective quantified approach to secure an organization, and finally iv) illustrate ii) and iii) using an example.

The rest of this paper is organized as follows. Section II discusses the nature of sensitive data and derives the estimates. Section III explains how the estimates are calculated and applied in a top-down quantified approach to secure an organization. Section IV presents an application example. Section V discusses related work. Finally, Section VI gives conclusions and future research.

II. Estimating Security Protection Levels

Before deriving estimates of security protection levels, it is useful to examine the nature of sensitive data.

A. Sensitive Data

We all have some sense of what is meant by sensitive data: first and foremost it is data that must be safeguarded from falling into the wrong hands, the consequence of which would be damaging to an individual or an organization. For an individual, sensitive data usually means private information. The nature of private information will not be explored here but the reader is encouraged to consult [2]. For an organization, sensitive data may encompass private information, but may additionally include information that may compromise the competitiveness of a company if divulged, such as trade secrets or proprietary algorithms and secret formulas. For this work, sensitive data is defined as follows:

DEFINITION 1: *Sensitive data* is information that must be protected from unauthorized access in order to safeguard the privacy of an individual or the operational well being of an organization.

This work considers losses arising from sensitive data or sensitive information being in the possession of unintended malicious parties or entities. This covers theft and any unintended exposure of sensitive information such as accidental leakage or posting. Per Definition 1, "sensitive data" and "sensitive information" are used interchangeably in this work. Some researchers make a distinction between these terms but the popular usage calls for no distinction.

A. Attacks on Organizations

Attacks carried out against sensitive information residing with organizations may be categorized as "outside attacks" and "inside attacks". We define these as follows.

DEFINITION 2: An *attack* is any action carried out against sensitive information held by an organization that, if successful, results in that information being in the hands of the attacker. An *outside attack* (A_o) is an attack that is carried out by an outsider of the organization (i.e., the attacker is not associated with the organization in a way that gives her special access privileges to sensitive data, e.g., a regular member of the public). An *inside attack* (A_i) is an attack that is carried out by an insider of the organization (i.e., someone who has special access privileges to sensitive data by virtue of her association with the organization, e.g., employee).

DEFINITION 3: A *vulnerability* of an organization is any weakness in the organization's infrastructure, platform, or business processes that can be targeted by an attack. A *secured-vulnerability* was originally a vulnerability that has had protective security measures put in place so that it is no longer a vulnerability. For example, a vulnerability is private information stored in the clear. This becomes a secured vulnerability if the private information is encrypted.

Outside attacks target a range of security vulnerabilities, from software systems that can be breached to access the sensitive information to simple theft of laptops and other devices used to store sensitive information. An example of an outside attack is the use of a Trojan horse planted inside the organization's computer system to steal sensitive information.

Inside attacks arise from the attacker making use of her privileged position (e.g., as an employee) to cause a loss of sensitive data. In this case, the attack is often difficult to detect, since it would appear as part of the normal duties of the insider attacker. An example of an inside attack is where a disgruntled employee secretly posts the organization's sensitive information on the Internet to try to harm the organization. An inside attack can also be unintentional (e.g., an employee casually providing client names for a survey).

Both outside and inside attacks target the organization's vulnerabilities. Vulnerabilities that invite outside attacks include the use of badly provisioned firewalls, the failure to encrypt data, and simple carelessness (e.g., leaving a laptop containing sensitive information in a car). Vulnerabilities that attract inside attacks include a) poor business processes that lack mechanisms to track which data is used where, used for what purpose, and accessed by whom, b) poor working conditions that give rise to employees feeling unfairly treated by management which can lead to employees seeking revenge, and c) poor education and enforcement of company policies regarding the proper care and handling of sensitive information (e.g., the above survey example).

We have so far used the expressions "level of protection" and "protection level" informally relying on their everyday meaning. We now formalize this meaning in terms of vulnerabilities, introducing the idea of "security protection level".

DEFINITION 4: An organization's security protection level (SPL) is the degree of security protection from attacks that results from the organization having secured q vulnerabilities, leaving p vulnerabilities unsecured, where the organization has a total of $p+q$ vulnerabilities. Each pair of values (p, q) corresponds to a different SPL.

B. Deriving the Estimates

Intuitively, for the same organization, SPL A is more capable of protecting from sensitive information loss than SPL B if A is composed of more secured vulnerabilities than B, where all vulnerabilities have roughly the same level of loss risk. This is the idea behind the derivation below.

We seek the capability C of an organization's SPL to protect sensitive data. Suppose that an organization's SPL has p vulnerabilities and q secured-vulnerabilities, where no distinction is made between outside and inside attacks. The number of original vulnerabilities before any vulnerabilities

ISBN: 978-1-61208-582-1

were secured is $p+q$. Let $P(e)$ represent the probability of event e. For convenience, "data" is understood to be "sensitive data". We have

$$C = P(\text{no data losses}) = 1\text{-}P(\text{data losses}) \tag{1}$$

Since a data loss is the result of a successful attack on a vulnerability,

$$P(\text{data losses}) \approx p/(p+q) \tag{2}$$

where we have applied the additive rule for the union of probabilities of attacks on the p vulnerabilities, assuming that 2 or more attacks do not occur simultaneously. This is a fair assumption confirmed by experience. Substituting (2) into (1) and adjusting for a possible zero denominator gives

$$C \approx 1\text{-}[p/(p+q)] = q/(p+q) \quad \text{if } p+q > 0 \tag{3}$$
$$= 1 \quad \text{if } p+q = 0 \tag{4}$$

Since C is a probability, its value is between 0 and 1, attaining 0 if the organization has no secured vulnerabilities ($q=0$, (3)) and 1 if either all of its vulnerabilities are secured ($p=0$, (3)) or if the organization has no vulnerabilities ($p+q=0$, (4)). Since an organization having no vulnerabilities is highly improbable, (4) is unlikely to apply.

The above derivation can be done within each of the categories of outside attacks and inside attacks (we did not distinguish between outside and inside attacks above). Let C_o, C_i represent the capabilities of an organization's SPL to protect sensitive information from outside attacks and inside attacks, respectively. Let p_o, p_i represent the number of vulnerabilities to outside attacks and inside attacks, respectively. Let q_o, q_i represent the number of secured vulnerabilities to outside attacks and inside attacks, respectively. Then, repeating the above derivation for outside attacks and inside attacks gives

$$C_o \approx q_o/(p_o+q_o) \quad \text{if } p_o+q_o > 0 \tag{5}$$
$$\approx 1 \quad \text{if } p_o+q_o = 0 \tag{6}$$
$$C_i \approx q_i/(p_i+q_i) \quad \text{if } p_i+q_i > 0 \tag{7}$$
$$\approx 1 \quad \text{if } p_i+q_i = 0 \tag{8}$$

As above, C_o (C_i) have values between 0 and 1, attaining 0 if the organization has no secured vulnerabilities to outside (inside) attacks ((5) and (7)) and 1 if either all of the vulnerabilities are secured ((5) and (7)) or if the organization has no vulnerabilities ((6) and (8)). Since an organization having no vulnerabilities to outside and inside attacks is highly improbable, (6) and (8) are unlikely to apply.

The estimates of data protection capability are now assigned as follows for a given SPL. Let E be an estimate of data protection capability, where no distinction is made between outside and inside attacks. Let E_o be an estimate of data protection capability against outside attacks. Let E_i be an estimate of data protection capability against inside attacks. Then for the SPL,

$$E = q/(p+q) \quad \text{if } p+q > 0 \tag{9}$$
$$= 1 \quad \text{if } p+q = 0 \tag{10}$$
$$E_o = q_o/(p_o+q_o) \quad \text{if } p_o+q_o > 0 \tag{11}$$
$$= 1 \quad \text{if } p_o+q_o = 0 \tag{12}$$
$$E_i = q_i/(p_i+q_i) \quad \text{if } p_i+q_i > 0 \tag{13}$$
$$= 1 \quad \text{if } p_i+q_i = 0 \tag{14}$$

E has the advantage of providing a single number for ease of comparison between different SPLs within an organization. A threshold T for E may be pre-determined such that for E above T, the security measures installed by the organization to secure vulnerabilities against both outside and inside attacks (corresponding to a SPL) are deemed adequate. For a given SPL, E_o *and* E_i have the advantage of focusing in separately on where an organization stands in terms of its security measures against outside and inside attacks. Thresholds T_o and T_i may be pre-determined for E_o and E_i respectively, such that for both estimates above their respective thresholds, the corresponding installed security measures against outside and inside attacks are deemed adequate. If this is the case, we call the corresponding SPL an *adequate SPL*. In practice, E_o and E_i may be expressed as percentages that define a region in a 100 x 100 plane in which an organization's capability to protect data is adequate (acceptable), as represented by the shaded region in Figure 1. Each point in this shaded region corresponds to an adequate SPL. An organization strives to have the "best" adequate SPL (one which has highest number of security measures possible against both outside and inside attacks) as allowed by its financial budget for adding security measures (see Section III).

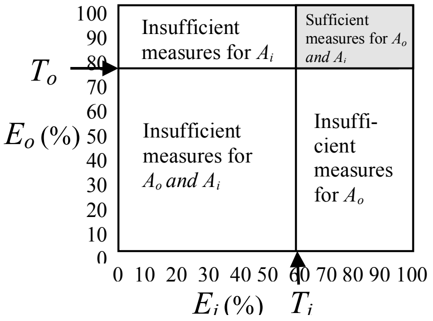
100
90
80
70
60
50
40
30
20
10
0
T_o
E_o (%)
Insufficient measures for A_i
Sufficient measures for A_o and A_i
Insufficient measures for A_o and A_i
Insuffi-cient measures for A_o
0 10 20 30 40 50 60 70 80 90 100
E_i (%)
T_i

Figure 1. Sufficiency of Security Measures Against Outside Attacks (A_o) and Inside Attacks (A_i)

III. APPLYING THE ESTIMATES TO OBTAIN A SPL

This section shows how an organization may use the estimates to establish a "best" adequate SDL as permitted by its financial budget. The description below separates outside attacks from inside attacks since organizations would need to account for them separately.

A. *Determining the Vulnerabilities*

For outside attacks, we recommend a threat analysis of security vulnerabilities in the organization's systems that could allow outside attacks to occur. The threat analysis can be carried out by a project team consisting of a security analyst, a privacy analyst, and a project leader acting as a facilitator. In addition to having expertise on privacy and security, the analysts must also be very familiar with the organization's systems. Threat analysis or threat modeling is a method for systematically assessing and documenting the security risks associated with a system (Salter et al. [3]).

Threat modeling involves understanding the adversary's goals in attacking the system based on the system's assets of interest. It is predicated on that fact that an adversary cannot attack a system without a way of supplying it with data or otherwise accessing it. In addition, an adversary will only attack a system if it has some assets of interest. The method of threat analysis given in [3] or any other method of threat analysis will yield $N_{\boldsymbol{o}} = p_o + q_o$, which is the total number of vulnerabilities to outside attacks. We will not take up room to provide further details on threat analysis here.

For inside attacks, we recommend that the above project team carry out a special insider threat analysis, to identify vulnerabilities to inside attacks and identify measures to secure these vulnerabilities. The team would accomplish this by brainstorming answers to the questions in Table 1, or other questions from experience, identifying the vulnerabilities and measures to secure the vulnerabilities in the process. In Table 1, questions 1 to 6 address motivational or environmental vulnerabilities, which may also be "secured" by applying mitigating measures. Questions 7 and 8 address security vulnerabilities. In identifying vulnerabilities to inside attack, the project team may weigh the vulnerabilities in terms of how likely they are to lead to attacks, and eliminate the unlikely ones. The weighing process may consider such factors as risk to the attacker that she could be caught as well as her motivation for the attack. The value of $N_{\boldsymbol{i}} = p_i + q_i$ would be determined at the end of this process.

B. *Determining the Thresholds T_o and T_i*

The values of T_o and T_i should be determined by the same threat analysis team mentioned above. The values would depend on the following:

- The potential value of the sensitive data – the more valuable the data is to a thief, a malicious entity, or a competitor, the higher the thresholds should be.
- The damages to the organization that would result, if the sensitive data were compromised – of course, the higher the damages, the higher the thresholds.
- The current and likely future attack climate – consider the volume of attacks and the nature of the victims, say over the last 6 months; if the organization's sector or industry has sustained a large number of recent attacks, then these thresholds need to be higher.
- Consider also potential attacks by nation states as a result of the political climate; attacks by individual hacktivist groups such as Anonymous or WikiLeaks may also warrant attention.

In general, an organization would like to be as secure as possible and establish a "best" adequate SPL. Therefore, values above 80% would not be uncommon. However, whatever the thresholds, the organization must find them acceptable after considering the above factors. It must also be kept in mind that the higher the thresholds, the higher will be the financial costs of implementing the security measures.

TABLE 1. QUESTIONNAIRE TO IDENTIFY VULNERABILITIES TO INSIDE ATTACK

	Question	Rationale
1.	Is the sensitive information of high value to outside agencies or a competitor?	The higher the value, the more an inside attacker will be tempted to steal and sell the information.
2.	Does the organization have an employee assistance program that includes counselling and help with financial difficulties?	Such a program may eliminate some financial motivation for an inside attack.
3.	Does the organization have an ombudsman or other impartial agent to assist employees with their grievances?	Such an impartial agent may eliminate or reduce the motivation to seek revenge by committing an inside attack.
4.	Does the organization have a history of perceived injustices to employees?	If the answer is 'yes', employees may be motivated by revenge to commit an inside attack.
5.	Does the organization conduct a stringent background and reliability check on a candidate for employment prior to hiring the candidate?	While a background and reliability check is not guaranteed to weed out potential inside attackers, it should eliminate those with criminal pasts.
6.	Does the organization require candidates for employment to disclose any potential conflicts of interest they may have with respect to their new employment and any outside interests prior to hire? Does the organization require ongoing disclosure of conflicts of interest after hire?	Eliminating conflicts of interest should reduce related motivations for malicious inside attacks. For example, an inside attacker may secretly compromise private information in favour of an outside interest, believing that the compromise is undetected.
7.	What are some possible ways for an insider to gain access to sensitive information she should not be accessing? How to secure?	This question will identify security weaknesses.
8.	What are some possible ways for an insider to transmit sensitive information outside the organization undetected? How to secure?	This question will identify additional security weaknesses.

C. *Applying the Estimates for a "Best" Adequate SPL*

We now have values for the following: $N_o = p_o + q_o$, $N_i = p_i + q_i$ (Section IIIA), and T_o, T_i (Section IIIB). Rewriting (11) and (13) and using the ceiling function to avoid fractional numbers of secured vulnerabilities gives:

$$q_o = \lceil N_oE_o \rceil \qquad \text{where } T_o \le E_o \le 1 \qquad (15)$$
$$q_i = \lceil N_iE_i \rceil \qquad \text{where } T_i \le E_i \le 1 \qquad (16)$$

Equations (15) and (16) give all possible values of q_o and q_i such that the associated E_o and E_i (with $p_o = N_o - q_o$ and $p_i = N_i - q_i$) fall within the shaded region of Figure 1. In other words, these equations give all possible values of q_o and q_i for adequate SPLs. The ceiling function biases the security level upward by taking the number of secured vulnerabilities to the next higher integer where applicable, which should be fine since more security should be better than less security. The quantities $q_o = \lceil N_oT_o \rceil$ and $q_i = \lceil N_iT_i \rceil$ from (15) and (16), termed respectively the threshold q_o and the threshold q_i, will be useful below.

To obtain a "best" adequate SPL from among the adequate SPLs generated by (15) and (16), the organization applies the constraint that the total cost of implementing the $(q_o + q_i)$ security measures from (15) and (16) must be less than or equal to the financial budget for security measures. The organization separately prioritizes its outside attack and inside attack vulnerabilities, and then selects them for securing in order of high priority to low priority, until both the financial budget is exhausted and the number of secured vulnerabilities are at least as great as the threshold q_o and the threshold q_i. In this way, the organization determines the q_o and q_i, as well as the p_o and p_i (which are just N_o - q_o and $N_i - q_i$ respectively) that define its "best" adequate SPL. This procedure may be precisely described as follows. Let $u_1, u_2, \ldots u_{No}$ and $v_1, v_2, \ldots v_{Ni}$ be the organization's prioritized outside attack and inside attack vulnerabilities, respectively, such that u_1 has higher (or equal) priority than u_2, u_2 has higher (or equal) priority than u_3, and so on. Similarly, v_1 has higher (or equal) priority than v_2, v_2 has higher (or equal) priority than v_3, and so on. Let B_o and B_i represent the budgets for securing against outside and inside attacks, respectively. Let C_o and C_i be the costs of securing the vulnerabilities to outside and inside attacks respectively. Let k be a counter variable. Then the pseudo code shown in Figure 2 describes the procedure for obtaining a "best" adequate SPL. Running this pseudo code will produce the following: a) q_o and q_i, defining the "best" adequate SPL, or b) one or two "insufficient budget" messages, in which case the organization has to increase the corresponding budgets and re-run the procedure. Only result a) would be acceptable.

Prioritizing the vulnerabilities may be based on four aspects of an attack, namely "risk", "access", "cost", and the resulting damages from the attack, where "risk" is risk to the safety of the attacker, "access" is the ease with which the attacker can access the system under attack, "cost" is the monetary cost to the attacker to mount the attack, and resulting damages is self evident. A full explanation of this prioritization procedure is given in Yee [2].

IV. APPLICATION EXAMPLE

Alice Inc., an online seller of goods (e.g., Amazon.com), has an objective to secure its vulnerabilities to outside and inside attacks and to establish a "best" adequate SPL using the approach in this work. The company hired a security consulting firm to perform threat analyses of its systems, resulting in a report of vulnerabilities found that could be targeted by outside and inside attackers. The report also provides values for the number of vulnerabilities as $N_o = 10$ and $N_i = 8$, and includes prioritizations of outside and inside vulnerabilities. For each type of vulnerability (i.e., outside or inside) the prioritizations identified which vulnerability required securing first, which one second, and so on, in declining order of urgency. Based on the consultant's recommendations, as well as its own internal deliberations, Alice Inc. assigned the following values:

```
Begin;
    $C_o = 0; C_i = 0; k = 0;$
    While $k \le N_o$ and $C_o \le B_o$;
        $k = k + 1;$
        $C_o = C_o$ + cost of securing $u_k$;
    EndWhile;
    If ($k \ge$ threshold $q_o$) $q_o = k$;
    Else Print "$q_o$ unavailable -insufficient budget";
    $k = 0;$
    While $k \le N_i$ and $C_i \le B_i$;
        $k = k + 1;$
        $C_i = C_i$ + cost of securing $v_k$;
    EndWhile;
    If ($k \ge$ threshold $q_i$) $q_i = k$;
    Else Print "$q_i$ unavailable – insufficient budget";
End;
```

Figure 2. Procedure for obtaining a "best" adequate SPL.

$$T_o = 0.80,\ T_i = 0.90,\ B_o = \$100{,}000,\ B_i = \$150{,}000$$

Therefore

threshold $q_o = \lceil N_oT_o \rceil = \lceil 10 \text{ x } 0.80 \rceil = 8$
threshold $q_i = \lceil N_iT_i \rceil = \lceil 8 \text{ x } 0.85 \rceil = 7$

meaning that at least 8 vulnerabilities to outside attacks and 7 vulnerabilities to inside attacks must be secured in order to have a "best" adequate SPL. Table 2 identifies the costs of securing the prioritized vulnerabilities where vulnerability 1 is the most urgent, vulnerability 2 is next urgent, and so on.

TABLE 2. COSTS OF SECURING OUTSIDE AND INSIDE VULNERABILITIES

u_k	Cost of Securing	v_k	Cost of Securing
1	$20,000	1	$40,000
2	$15,000	2	$40,000
3	$10,000	3	$30,000
4	$10,000	4	$20,000
5	$8,000	5	$10,000
6	$7,000	6	$5,000
7	$5,000	7	$5,000
8	$5,000	8	$5,000
9	$3,000		
10	$2,000		

As in Section III, outside and inside vulnerabilities are denoted as u_k *and* v_k respectively. Running the pseudo code in Figure 2 yields $C_o = \$85{,}000$ at $q_o = 10$ and $C_i =$

\$150,000 at $q_i = 7$. The budget for securing outside vulnerabilities was more than enough to secure all outside vulnerabilities. The budget for securing inside vulnerabilities was only enough to secure 7 inside vulnerabilities. Given the existing budgets, Alice Inc.'s "best" adequate SPL is realized with $q_o = 10, p_o = 0$ *and* $q_i = 7, p_i = 1$. Any additional security measure against inside attacks would require an increase in the budget.

V. RELATED WORK

Related work found in the literature includes risk and threat analysis applied to various domains as well as research on vulnerabilities. No other work was found that is similar to this work.

In terms of risk analysis, Jing et al. [4] present an approach that uses machine learning to continuously and automatically assess privacy risks incurred by users of mobile applications. Aditya et al. [5] catalog privacy threats introduced by new, sophisticated mobile devices and applications. Their work emphasizes how these new threats are fundamentally different and inherently more dangerous than prior systems, and present a new protocol for secure communications between mobile devices.

In terms of threat analysis, Schaad and Borozdin [6] present an approach for automated threat analysis of software architecture diagrams. Their work shows that automated threat analysis is feasible. Shi et al. [7] describe a hybrid static-dynamic approach for mobile security threat analysis, where the dynamic part executes the program in a limited way by following the critical path identified in the static part. Sanzgiri and Dasgupta [8] summarize and classify insider threat detection techniques based on the detection strategies used. Sokolowski and Banks [9] describe the implementation of an agent-based simulation model designed to capture insider threat behavior, given a set of assumptions governing agent behavior that predisposes an agent to becoming a threat.

With regard to vulnerabilities, Gawron et al. [10] investigate the detection of vulnerabilities in computer systems and computer networks. They use a logical representation of preconditions and postconditions of vulnerabilities, with the aim of providing security advisories and enhanced diagnostics for the system. Spanos et al. [11] look at ways to improve the open standard to score and rank vulnerabilities, known as the Common Vulnerability Scoring System (CVSS). They propose a new vulnerability scoring system called the Weighted Impact Vulnerability Scoring System (WIVSS) that incorporates the different impact of vulnerability characteristics. In addition, the MITRE Corporation maintains the Common Vulnerability and Exposures (CVE) list of vulnerabilities and exposures [12], standardized to facilitate information sharing.

VI. CONCLUSIONS AND FUTURE RESEARCH

Organizations need to protect their sensitive data from outside and inside attacks against their computer systems that store the data. This protection is achieved by adding security measures to secure vulnerabilities to attack. However, organizations have been implementing security measures without any way of setting security protection level targets, or knowing how an added security measure contributes to the protection target. Organizations also did not have a way of selecting which security measures to implement in order to stay within the financial budget. This work proposes a quantitative approach to estimate, set, and achieve safe security protection levels in terms of securing outside and inside vulnerabilities. In addition, the work proposes a procedure for selecting which security measures to implement in order to achieve targeted protection levels within the allowable financial budget.

Future research includes investigating other formulations of security protection levels, such as incorporating the effectiveness of security measures, as well as improving the methods for threat analysis and prioritization. In addition, it would be interesting to explore how this work complements existing work in the standardization community.

REFERENCES

[1] Identity Force, "The Biggest Data Breaches in 2016," retrieved: July, 2017, https://www.identityforce.com/blog/2016-data-breaches

[2] G. Yee, "Visualization and Prioritization of Privacy Risks in Software Systems," International Journal on Advances in Security, issn 1942-2636, vol. 10, no. 1&2, pp. 14-25, 2017, http://www.iariajournals.org/security/

[3] C. Salter, O. Saydjari, B. Schneier, and J. Wallner, "Towards a Secure System Engineering Methodology," Proc. New Security Paradigms Workshop, pp. 2-10, 1998.

[4] Y. Jing, G.-J. Ahn, Z. Zhao, and H. Hu, "RiskMon: Continuous and Automated Risk Assessment of Mobile Applications," Proc. 4th ACM Conference on Data and Application Security and Privacy (CODASPY '14), pp. 99-110, 2014.

[5] P. Aditya, B. Bhattacharjee, P. Druschel, V. Erdélyi, and M. Lentz, "Brave New World: Privacy Risks for Mobile Users," Proc. ACM MobiCom Workshop on Security and Privacy in Mobile Environments (SPME '14), pp. 7-12, 2014.

[6] A. Schaad and M. Borozdin, "TAM2: Automated Threat Analysis," Proc. 27th Annual ACM Symposium on Applied Computing (SAC '12), pp. 1103-1108, 2012.

[7] Y. Shi, W. You, K. Qian, P. Bhattacharya, and Y. Qian, "A Hybrid Analysis for Mobile Security Threat Detection," Proc. IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 1-7, 2016.

[8] A. Sanzgiri and D. Dasgupta, "Classification of Insider Threat Detection Techniques," Proc. 11th Annual Cyber and Information Security Research Conference (CISRC '16), article no. 25, pp. 1-4, 2016.

[9] J. Sokolowski and C. Banks, "An Agent-Based Approach to Modeling Insider Threat," Proc. Symposium on Agent-Directed Simulation (ADS '15), pp. 36-41, 2015.

[10] M. Gawron, A. Amirkhanyan, F. Cheng, and C. Meinel, "Automatic Vulnerability Detection for Weakness Visualization and Advisory Creation," Proc. 8th International Conference on Security of Information and Networks (SIN '15), pp. 229-236, 2015.

[11] G. Spanos, A. Sioziou, and L. Angelis, "WIVSS: A New Methodology for Scoring Information System Vulnerabilities," Proc. 17th Panhellenic Conference on Informatics, pp. 83-90, 2013.

[12] MITRE, "Common Vulnerabilities and Exposures", retrieved: July, 2017, https://cve.mitre.org/

ISBN: 978-1-61208-582-1