Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility

Ferenc Leitold
Secudit, University of Dunaújváros

Anthony Arrott
Secudit

Kálmán Hadarics
Secudit, University of Dunaújváros

Abstract

An integrated measure of cyber-threat vulnerability is presented that accounts for three disparate but interrelated sources of vulnerability: attacker ingenuity, infrastructure weakness, and adverse user behavior. General analytical formulas for assessing risk dependent on three interrelated variables are applied to the cybersecurity endpoint protection problem. More narrowly, we focus on endpoint vulnerability to broad spectrum malware and phishing attacks. For any given cyber-threat or aggregated class of cyber-threats for which the requisite IT infrastructure vulnerability and user facilitation is known, we can obtain a best estimate of: (1) The probability that an attacker will use a particular threat or class of threats against the enterprise; (2) The probability that the enterprise's IT infrastructure will allow the attack to be carried out successfully; and (3) The probability that users of the enterprise's IT infrastructure will provide sufficient facilitation for the attack to succeed. These three probabilities can be combined to obtain an overall probability of malicious success, (provided each relevant combination of attack, user, and component of IT infrastructure is accounted for). Separately measured probabilities of malicious success can be combined, compared and prioritized. Subsequently, identified high priority vulnerabilities can be decomposed into constituent vulnerability sources allowing remedial actions to be directed where the greatest measureable improvement can be made.

Introduction

To succeed, a malware attack directed against a protected target network requires successful execution of the malicious code by the protected IT with sufficient authorized user facilitation to subvert the network security. Minimally, user facilitation may be as simple as having the endpoint device powered on and connected to the Internet. Cybersecurity metrics have tended to focus on protected IT (e.g., ongoing penetration testing) [28] and malicious activity (e.g., breach detection testing) [12]. User behavior cybersecurity metrics are less developed [9], although network traffic monitoring provides rich opportunities for their development (e.g., NetFlow/IPFIX) [27]. In addition to passive monitoring, interactive metrics can also be deployed [20], for example, probing user responses with fake phishing [8].

From a defender viewpoint, successful malicious attacks can be conceptually represented as occurring at the intersection of malicious activity acting on protected IT infrastructure, facilitated by sufficient authorized user behavior (Figure 1). This conceptual framework builds on the operational formulation used by NSS Labs [13, 30]. It is intended as a practical and convenient simplification of a more rigorous and complete treatment of attack surfaces [23]. Here we are focused exclusively

on human-interactive endpoints (IT) as opposed to the security architecture of embedded systems (IoT, OT) [32]. For our purposes here, three distinct but highly interactive sources of vulnerability are considered:

(1) Malicious activity by those who would subvert network capabilities for their own gain in violation of intended trusted relationships within the protected IT network;

(2) Disruptive and dangerous IT behaviors by network users (e.g., employees, customers, suppliers) in using IT network capabilities; and

(3) Unprotected vulnerabilities in the IT network infrastructure.

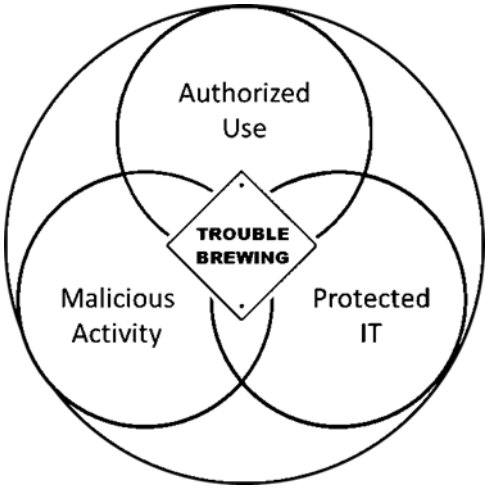

Figure 1: Cybersecurity incidents are most likely to arise when malicious activity subverts authorized use of vulnerable (e.g., unpatched) IT infrastructure.

The most critical vulnerabilities in IT networks lie at the intersection of these three areas (Figure 1). Addressing these vulnerabilities requires sufficient visibility, scrutiny and discrimination to observe, understand, and take effective action to mitigate them. Visibility of present and emerging vulnerability is most effectively achieved by vigilance in an ongoing risk analysis that combines observations in each of the three areas (Figure 2).

Figure 2: Components and contributing factors to IT network vulnerability can be segmented into three areas each of which has its own sets of methods and tools for visibility, scrutiny, and discrimination.

Visibility into information transaction vulnerabilities that threaten the wellbeing of an enterprise is a necessary but, by itself, completely insufficient requirement for enterprise cybersecurity. Vulnerability assessment may be thought of as the outermost layer in the ongoing provision of enterprise cybersecurity. The succeeding layers include: vulnerability detection, vulnerability

remediation, security incident preparedness, security incident detection, and security incident response (Figure 3).

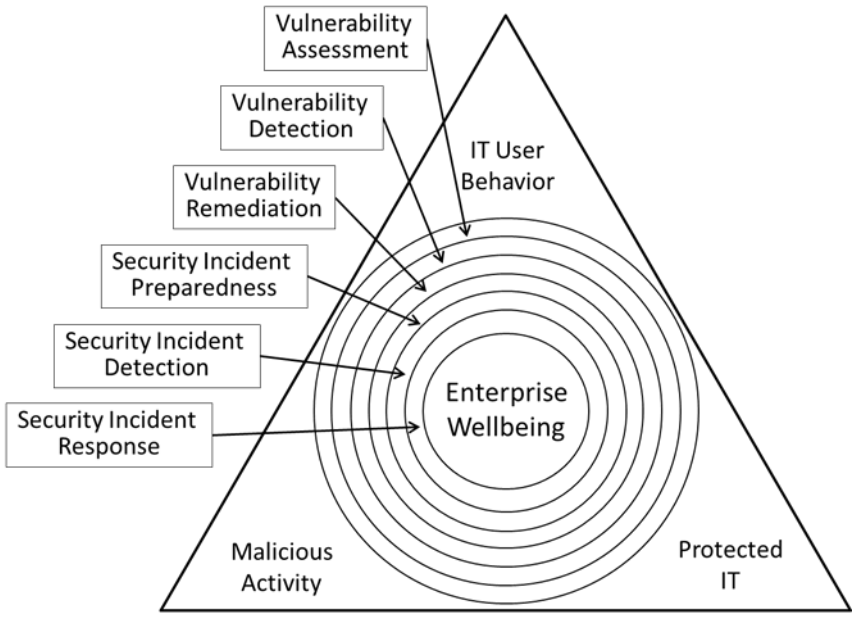

Figure 3: Vulnerability assessment within the context of overall cybersecurity contribution to enterprise wellbeing.

To effectively contribute to enterprise wellbeing, vulnerability management requires practical and useful correlation of the various and highly interactive sources of vulnerability. The analogous requirement for security incident response is typically satisfied by security event information management systems (SEIM) [31]. For vulnerability management, we have adopted what we define as the Triunal Model of Cybersecurity Vulnerability. Derived from earlier formulations [21, 22], the triunal model decomposes vulnerability assessment into three contributing sources, or triunes: i) malicious activity; ii) unprotected IT; and iii) facilitating adverse user behavior. Within each contributing source, specific contributing factors are identified and characterized (e.g., social engineering and exploits within the malicious activity triune). The model provides a basis for correlating and combining contributing factors into an integrated view of specific vulnerabilities [57].

First Triune: Malicious Activity by Threat Actors

We first consider malicious activity by those who would subvert network capabilities for their own gain in violation of intended trusted relationships within the protected IT network. Cybersecurity in this area is largely achieved through prevention, detection, and deflection of malware attacks using commercially-available automated software applications and appliances.

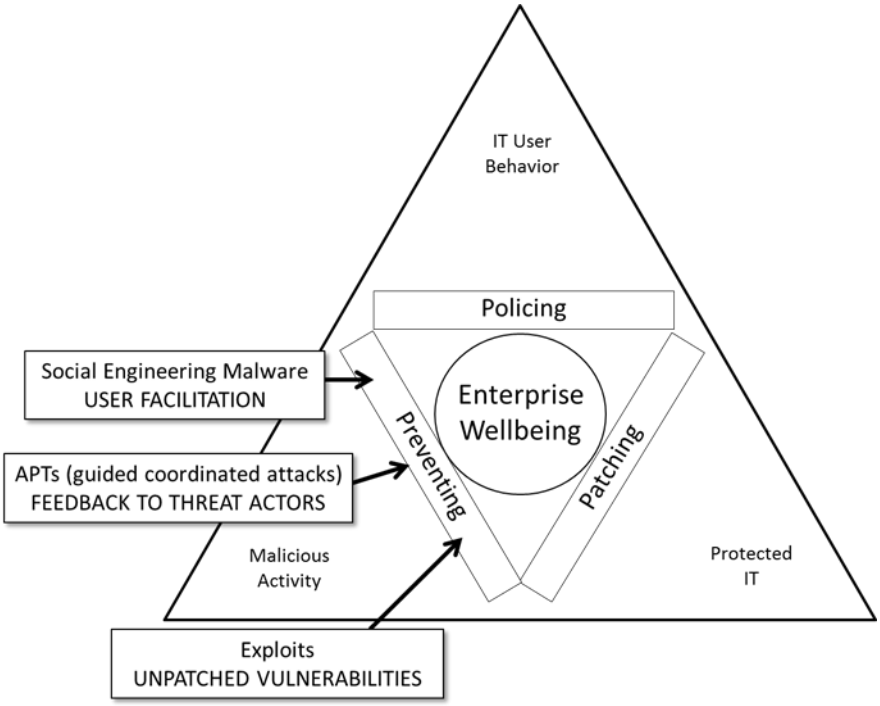

Figure 4: Typical sources of malicious activity vulnerabilities.

Malicious activity typically focuses on attack prevention weaknesses in the target victim's IT network and usage in the form of: (i) user facilitation (social engineering malware); (ii) feedback to threat actors from within the organization network (guided coordinated attacks, aka APTs); and (iii) malicious exploits of known & unknown vulnerabilities (Figure 4). Available methods for measuring vulnerabilities include malware susceptibility testing, breach detection testing, and exploit advance warning (Table 1).

Preventing	Malicious Activity Vulnerabilities		
	threat-enabling mechanism	root vulnerability	vulnerability assessment methodology
	Social Engineering Malware	User Facilitation	Malware Susceptibility Testing
	APTs (guided coordinated attacks)	Feedback to Threat Actors	Breach Detectability Testing
	Exploits	Unpatched Vulnerabilities	Exploit Advance Warning

Table 1: Malicious activity vulnerability assessment.

Second Triune: Deployed IT Network Vulnerabilities

Secondly, we consider unprotected vulnerabilities in an enterprise's deployed IT network infrastructure. This includes both the traditional concept of a walled network with controllable gateways as well as all the extended networks that inter-penetrate the enterprise network (largely due to mobility and cloud services) [11]. Cybersecurity in this area is largely achieved through vigilant IT network maintenance and effective operation including up-to-date patching and upgrading of component IT infrastructure.

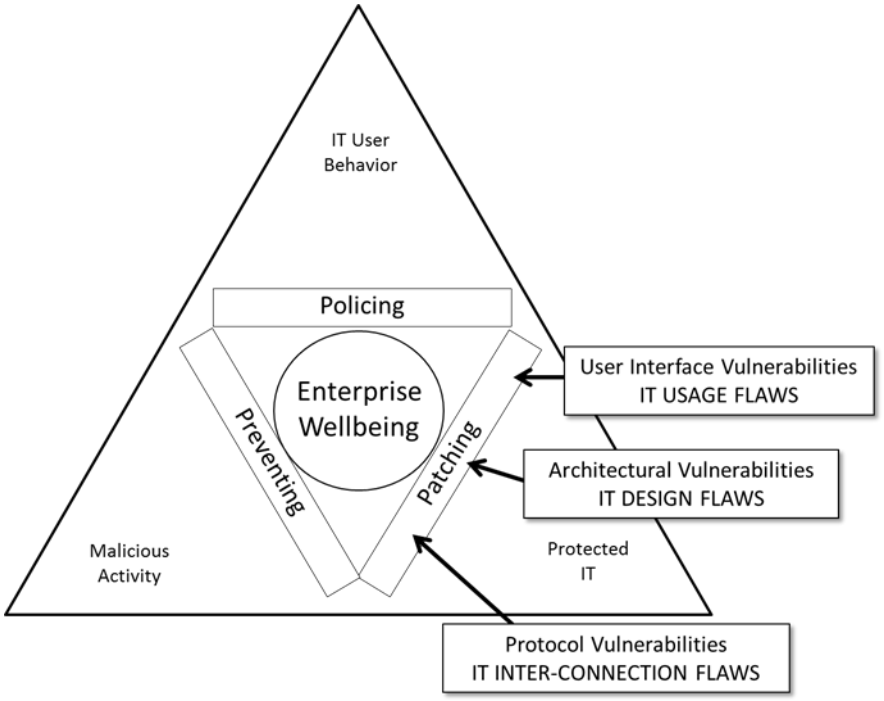

Figure 5: Typical sources of IT network infrastructure vulnerabilities.

Unprotected IT infrastructure vulnerabilities typically appear as system and applications patching shortcomings in the form of: (i) user interface vulnerabilities (IT usage flaws); (ii) IT architectural vulnerabilities (IT design flaws); (iii) protocol vulnerabilities (IT interconnection flaws) (Figure 5). Available methods for measuring IT infrastructure vulnerability include penetration testing, application security testing, and port scanning (Table 2)

Patching	Deployed IT Vulnerabilities		
	threat-enabling mechanism	root vulnerability	vulnerability assessment methodology
	User Interface Vulnerabilities	IT Usage Flaws	Penetration Testing
	Architectural Vulnerabilities	IT Design Flaws	Application Security Testing
	Protocol Vulnerabilities	IT Inter-connection Flaws	Port Scanning

Table 2: IT infrastructure vulnerability.

Third Triune: User Behavior Vulnerabilities

Finally, we consider vulnerabilities due to disruptive and dangerous IT behaviors by the users of enterprise IT network capabilities. Cybersecurity in this area is largely achieved through policy which is implemented and maintained primarily through training, security awareness, identity privilege management, and user behavior monitoring.

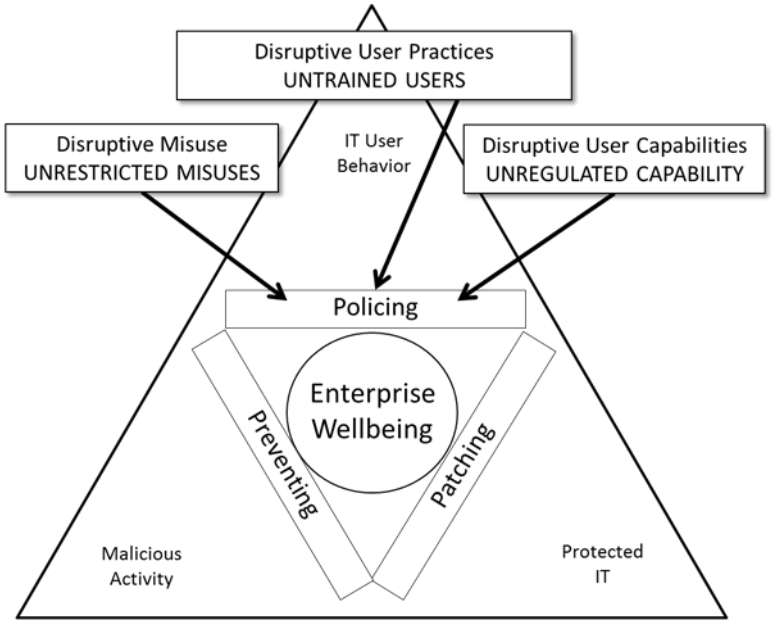

Figure 6: Typical sources of user behavior vulnerabilities.

Disruptive and dangerous usage of IT networks typically appears as anomalies in baseline (normative) user behaviors in the form of: (i) unrestricted misuses; (ii) untrained and naïve user behaviors; (iii) unregulated user capabilities (Figure 6). Available methods for measuring IT user behavior vulnerabilities include access control testing, user proficiency assessment, and behavior anomaly detection (Table 3).

Policing	IT User Behavior Vulnerabilities		
	threat-enabling mechanism	root vulnerability	vulnerability assessment methodology
	Disruptive Misuse	Unrestricted Misuses	Access Control Testing
	Disruptive User Practices	Untrained Users	User Proficiency Assessment
	Disruptive User Capabilities	Unregulated Capability	Behavior Anomaly Detection

Table 3: User behavior vulnerability assessment.

Correlating and Combining Sources of Vulnerability

Let us define the followings:

L: set of all available threat landscapes (e.g.: World, Europe, USA, Hungary, …)

T_{all}: set of all possible malware

(note: at this moment we are focusing of the subset of threats, we are dealing with only the programmed attacks)

T_l: set of all possible malware inside $l \in L$, $T_l \subset T_{all}$

U: set of all users

I: set of all possible devices

P: set of all available protections

UT: set of all possible user tricks used by any malware in T

An integrated measure of vulnerability can be derived accounting for all three sources (attacker ingenuity, infrastructure weakness, adverse user behavior). For any given malware or class of malware for which the requisite IT infrastructure vulnerability and user facilitation is known, we can obtain a best estimate of:

1. The probability that an attacker will use a particular malware or class of malware against the enterprise (p_{prev}):

$$p_{prev}(t,l) = \frac{number\ of\ computers\ infected\ by\ \boldsymbol{t}\ inside\ \boldsymbol{l}}{number\ of\ all\ comupters\ inside\ \boldsymbol{l}}$$

where $t \in T_l$ and $l \in L$;

2. The probabilities that the enterprise's IT infrastructure will allow the attack to be carried out successfully (p_{device}):

$$p_{prot}(t,p) = \frac{number\ of\ successfull\ attempts\ of\ \boldsymbol{t}\ thru\ the\ protection\ \boldsymbol{p}}{number\ of\ all\ attempts\ of\ \boldsymbol{t}\ thru\ the\ protection\ \boldsymbol{p}}$$

where $t \in T_l, l \in L$ and $p \in P$;

$$p_{device-prot}(t,i) = \min_{for\ all\ p\ protecting\ i} p_{prot}(t,p)$$

where $t \in T_l, l \in L$ and $i \in I$;

$$p_{device-elements}(t,i) = \begin{cases} 1, if\ t\ can\ work\ on\ i \\ 0, if\ t\ can\ not\ work\ on\ i \end{cases}$$

where $t \in T_l, l \in L$ and $i \in I$;

$$p_{device}(t,i) = p_{device-elements}(t,i) \cdot p_{device-prot}(t,i)$$

where $t \in T_l, l \in L$ and $i \in I$;

3. The probability that users of the enterprise's IT infrastructure will provide sufficient facilitation for the attack to succeed ($p_{usertrick}$, p_{user}, p_{usage}):

$$p_{usertrick}(t,ut) = \frac{number\ of\ attempts\ of\ \boldsymbol{t}\ where\ t\ used\ \boldsymbol{ut}}{number\ of\ all\ attempts\ of\ \boldsymbol{t}}$$

where $t \in T_l, l \in L$, $ut \in UT$;

$$p_{user}(u, ut) = \frac{number\ of\ successfull\ attempts\ of\ \boldsymbol{ut}\ on\ \boldsymbol{u}}{number\ of\ all\ attempts\ of\ \boldsymbol{ut}\ on\ \boldsymbol{u}}$$

where $u \in U$, $ut \in UT$;

$$p_{usage}(u, i) = \frac{all\ time\ when\ u\ used\ i}{measuring\ interval}$$

where $u \in U$, $i \in I$;

The three main input classes (p_{prev}, p_{device}, $p_{usertrick}$ and p_{user}) can be combined to obtain an overall probability of malicious success (provided each relevant combination of attack, user, and component of IT infrastructure is accounted for):

$$q(l, i, ut) = 1 - \prod_{t}(1 - p_{usertrick}(t, ut) \cdot p_{prev}(t, l) \cdot p_{device}(t, i))$$

where $u \in U$, $i \in I$, $t \in T_l, l \in L$;

$$r(l, u, i) = 1 - \prod_{ut}(1 - q(l, i, ut) \cdot p_{user}(u, ut))$$

where $u \in U$, $i \in I, ut \in UT, l \in L$;

$$s(l) = 1 - \prod_{u,i}(1 - r(l, u, i) \cdot p_{usage}(u, i))$$

where $u \in U$, $i \in I$ and $l \in L$;

Separately measured combined probabilities of malicious success (p_{s1}, p_{s2}, p_{s3}, …) can be compared and prioritized. Subsequently, an identified high priority vulnerability (p_{si}) can be decomposed into its constituent vulnerability sources (p_{ai}, p_{bi}, p_{ci}) allowing remedial actions to be directed where the greatest measureable improvement can be made.

Table 4 provides descriptions of each of the elements in the equations above.

formula element	description
$t \in T$	Individual threat, t, member of the set of all threats, T, under consideration in the vulnerability assessment.
$i \in I$	Individual IT infrastructure element, i, member of the set of all IT infrastructure elements, I, under consideration in the vulnerability assessment.
$u \in U$	Individual user, u, member of the set of all users, U, under consideration in the vulnerability assessment.
$ut \in UT$	Individual threat, ut, member of the set of all threats, UT, under consideration in the vulnerability assessment.
$p_{prev}(t,l)$	Prevalence of threat t in the threat landscape l. The probability that the threat t tries to infect a device in the threat landscape l.
$p_{prot}(t,p)$	The probability that the protection p is unable to block the threat t.
$p_{device-prot}(t,i)$	The probability that none of the protections protecting i is able to block the threat t.
$p_{device-elements}(t,i)$	1, if the hardware and software settings of i are capable to execute the threat t, independently from any protection inside i.
$p_{device}(t,i)$	The probability that the threat t can be executed on i. (The elements of I are capable to run t and the protections can not block it.
$p_{usertrick}(t,ut)$	The probability that the threat t uses the usertrick ut during its single execution.
$p_{user}(u,ut)$	The probability that the user u executes the action required by the usertrick ut.
$p_{usage}(u,i)$	The probability that the user u uses the device i at the given moment.
$q(l,i,ut)$	The probability of any of the threats in the subset of threats of the threat landscape l using the given ut can reach i.
$r(l,u,i)$	The probability of any of the threats of the threat landscape reach i while u is using it.
$s(l)$	The probability of any of the threats of the threat landscape infect any device in the organization.

Table 4: List of formulae elements and their descriptions.

Synthetic Example

To illustrate the use of the formulae in the previous section, we present a simplified synthetic example. Consider an organization in which three users (Kim, Susan, Peter) have been characterized for their susceptibility to three social engineering techniques (user tricks X, Y, and Z). Further, consider five threats (A, B, C, D, E) of known prevalence in the organization's locale and among its peer group organizations. Assume the likelihood that each of these threats will employ any of the social engineering techniques (X, Y, Z) has been determined. Finally, we assume that the users are all using similarly-configured endpoint devices (e.g., Win7), each with similarly configured endpoint protection (e.g., similarly configured anti-malware applications). The sets considered in this example are summarized in Table 5.

sets	description	#	members
T	threats	5	{A, B, C, D, E}
U	users	3	{Kim, Susan, Peter}
I	infrastructure	1	{protected endpoint}

UT	user tricks	3	{X, Y, Z}

Table 5: Summary of sets in synthetic example.

The prevalence of each cyber-threat, the likelihood of its applicability to the organization's infrastructure, and the expected efficacy of the endpoint protection against each threat are summarized in Table 6.

	Threats				
	A	B	C	D	E
Prevalence	35%	24%	18%	15%	8%
Infrastructure applicability	11%	55%	55%	0%	100%
Protection efficacy	35%	80%	100%	15%	56%

Table 6: Threat prevalence, infrastructure applicability, and protection efficacy for each threat.

The likelihood for each cyber-threat to utilize each social engineering user trick is summarized in Table 7.

		Threats				
User Tricks		A	B	C	D	E
	X	100%	50%	0%	30%	20%
	Y	0%	0%	50%	80%	0%
	Z	0%	50%	70%	0%	100%

Table 7: Likelihood that each threat utilizes each social engineering user trick.

The likelihood for each cyber-threat to utilize each social engineering user trick is summarized in Table 8.

		Users		
		Kim	Susan	Peter
User Tricks	X	40%	70%	6%
	Y	30%	55%	2%
	Z	20%	60%	3%

Table 8: User susceptibility to each social engineering user trick.

The likelihood that each user's endpoint will be in use at any given time is summarized in Table 9.

	Users		
	Kim	Susan	Peter
Infrastructure Usage	50%	60%	55%

Table 9: Infrastructure usage by each user.

The output vulnerability probabilities are summarized in Table 10.

	User Tricks		
	X	Y	Z
q(ut)	22%	11%	25%
	Users		
	Kim	Susan	Peter
r(u)	16%	32%	2%
	Overall Vulnerability Metric		
s(u)	27%		

Table 10: Output metrics, q(ut), r(u), and s.

Actionable Quantification of Vulnerability

The output of applying the Triunal Model of Cybersecurity Vulnerability to a specific organization can be used to compare and prioritize specific sources of vulnerability within the organization. Using the results in the synthetic example above, we can compare vulnerabilities due to specific social engineering tricks with vulnerabilities due to the susceptibilities of each user to those tricks. We do this by assigning the total probability of social engineering success and user susceptibility across the three individual tricks (X, Y, Z) and the three users (Kim, Susan, Peter), respectively. As shown in Table 11, 43% of the vulnerability due to social engineering is concentrated in user trick Z, only marginally more than the vulnerability mass of user trick X (38%).

User Trick	X	Y	Z
probability, q(ut)	22%	11%	25%
vulnerability mass	38%	19%	43%

Table 11: Calculation of vulnerability masses for individual user tricks in the synthetic example. Vulnerability masses add to unity and are indicative of the relative vulnerability for each of the component sources.

In contrast, Table 12 shows the vulnerability mass attributable to user Susan (64%) is double the vulnerability mass of the next most vulnerable user (Kim at 32%).

User	Kim	Susan	Peter
probability, r(u)	16%	32%	2%
vulnerability mass	32%	64%	4%

Table 12: Calculation of vulnerability masses for individual users in the synthetic example. Vulnerability masses add to unity and are indicative of the relative vulnerability for each of the component sources.

Without further analysis, the following differential recommendation might be made regarding efforts to reduce cyber-threat vulnerability at the organization in the synthetic example:

"*All other things being equal, efforts to train user Susan to be less susceptible to social engineering cyber-threats will likely produce more overall cyber-security for the organization than efforts to make all users aware of social engineering user trick Z.*"

In any case for this synthetic example, distracting user Peter with social engineering susceptibility training would appear to be a waste of organization resources.

Conclusion

In this paper a method is presented for measuring the vulnerability of a specific organization to successful malicious attack from its current surrounding cyber-threat landscape. The method utilizes three sources of information: external cyber-threat intelligence ("security intelligence"), organization IT infrastructure weakness ("penetration testing"), and the susceptibility of the organization's IT users to facilitating cyber-attacks ("user behavior"). The method allows the measured sources of vulnerability to be systematically combined into a metric of overall vulnerability which can be decomposed into comparable contributing relative vulnerabilities from each source. The method quantifies the evolution of relative vulnerabilities over time, separately measures the vulnerability of individual departments (LANs) and to specific classes of cyber-threats (e.g., ransomware, phishing). In addition, the method predicts the consequences of potential remedial actions ("What ifs?"), thus aiding cyber-security decision-making specific to an organization's unique situation.

References

[1] AHN, Michael J., Tae-Hyung Park, and Chae-Hong Lim. "What Matters in Cybersecurity? The Role of Citizen Perception and Attributes." IJeN 3.1: 1-22. 2015.

[2] ARROTT, A., F. Lalonde Levesque, D. Batchelder, and J.M. Fernandez. "Citizen cyber-security health metrics for Windows computers". Proceedings of Eastern European eGov Days Conference, EEGOV, Budapest, Hungary. 2016.

[3] BATCHELDER, D., et al. "Microsoft Security Intelligence Report." Volume 18: July-December 2014, Microsoft, 2015.

[4] BERTOLLO, P. "Assessing ecosystem health in governed landscapes: a framework for developing core indicators". Ecosystem health, 4(1):33–51, 1998.

[5] BLACKBIRD, J. and B. Pfeifer. "The global impact of anti- malware protection state on infection rates". In Virus Bulletin Conf., 2013.

[6] BLIZARD, Tommy, and Nikola Livic. "Click-fraud monetizing malware: A survey and case study." Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on. IEEE, 2012.

[7] BRAVERMAN, M., "Behavioral modeling of social engineering-based malicious software". Virus Bulletin Conf., 2006.

[8] CHAPMAN M.T., "Advanced Persistent Testing: How to fight bad phishing with good." PhishLine, 2015.

http://www.phishline.com/advanced-persistent-testing-ebook

[9] CHAPMAN, M.T., "Establishing metrics to manage the human layer." ISSA Security Education Awareness Special Interest Group, 2013.

[10] CLEMENTI, Andreas, Peter Stelzhammer, and Fernando C. Colon Osorio. "Global and local prevalence weighting of missed attack sample impacts for endpoint security product comparative detection testing." Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on. IEEE, 2014.

[11] COLON OSORIO, F.C., and A. Arrott. "Fabric of security - changing our theory and expectations of modern security". Proceedings of Eastern European eGov Days Conference, EEGOV, Budapest, Hungary. 2016.

[12] EDWARDS, S.E., R. Ford, and G. Szappanos., "Effectively testing APT defenses". Virus Bulletin Conference, Prague, Czech Republic, 2015.

[13] FREI, S. "Vulnerability threat trends." NSS Labs, Austin, Texas. 2013.

http://nsslabs.com

[14] HARKNETT, Richard J., and James A. Stever. "The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen." Journal of Homeland Security and Emergency Management 6.1, 2009.

[15] HILBERT, M., "The maturing concept of e-democracy: from e-voting and online consultatons to democratic value out of jumbled online chatter". Journal of Information Technology and Politics, 6.2: 87-110. 2009.

[16] JORBA, A.R., J.A.O. Ruiz, and P. Brown. "Advanced security to enable trustworthy electronic voting." Third European Conference on e-Government. 2003.

[17] KLEINER, A., P. Nicholas, K. Sullivan, "Linking Cybersecurity Policy and Performance, Microsoft Trustworthy Computing", 2013,

[18] KSHETRI, Nir. "Cybercrime and Cybersecurity in the Middle East and North African Economies." Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan UK, 2013.

[19] LALONDE LEVESQUE, F., A. Somayaji, D. Batchelder, and J.M. Fernandez. "Measuring the health of antivirus ecosystems." Malicious and Unwanted Software (MALWARE), 2015 10th International Conference on. IEEE, 2015.

[20] LALONDE LEVESQUE, F., J. M. Fernandez, and A. Somayaji. "Risk prediction of malware victimization based on user behavior." Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on. IEEE, 2014.

[21] LEITOLD, F and K. Hadarics. "Measuring security risk in the cloud-enabled enterprise." Malicious and Unwanted Software (MALWARE), 7th International Conference on Malicious and Unwanted Software, pp: 62-66, ISBN: 978-1-4673-4880-5. 2012.

[22] LEITOLD, F. "Security Risk analysis using Markov Chain Model." 19th Annual EICAR Conference, Paris, France. 2010.

[23] MANDHATA P.K., J.M. Wing, "An Attack Surface Metric". IEEE Transactions on Software Engineering, 2010.

[24] MCCORMACK, Matt. "When the hammer falls – effects of successful widespread disinfection on malware development and direction." Virus Bulletin Conf., 2008.

[25] MICROSOFT. "Evolution of malware and the threat landscape - a 10-year review". 2012.

[26] MICROSOFT. "Malicious Software Removal Tool (MSRT) ". Microsoft Knowledge Base, article KB890830 revision 161.2,

https://support.microsoft.com/en-us/kb/890830

[27] PLIXER., "IPFIXify - Turn machine generated data into real-time visibility and insight". Whitepaper. 2014.

http://www.plixer.com

[28] PWNIE EXPRESS., "Vulnerability assessment and penetration testing across the enterprise". Whitepaper, 2014.

http://www.pwnieexpress.com

[29] RUBENKING N., "Why Microsoft Doesn't Need Independent Antivirus Lab Tests". PC Magazine, 28 October 2013.

http://securitywatch.pcmag.com/security-software/317280-why-microsoft-doesn-t-need-independent-antivirus-lab-tests

[30] SHAH P, Phatak V, Scipioni R, inventors. "Adaptive intrusion detection system." United States patent application US 10/443,568. 2003 May 22.

[31] SUAREZ-TANGIL G., E Palomar, A Ribagorda, Y Zhang. "Towards an intelligent security event information management system".

http://www.seg.inf.uc3m.es/papers/2013nova-AIS-SIEM.pdf

[32] URIBEETXEBERRIA R., MG Eskola, L Trono, S Galileo, JN Movation, L de Celis Acorde, A Morgani, ES Selex, R Baldelli, IE Tecnalia, NP Hai, "New embedded systems architecture for multi-layer dependable solutions".

http://www.newshield.eu/wp-content/uploads/2013/11/NSHIELD-D8.6_Build_Secure_Systems_with_SHIELD_v2.pdf