Optimal Level and Allocation of Cybersecurity Spending

By Shaun S. Wang

Editor's Note: The 52nd Actuarial Research Conference (ARC) was held in Atlanta in July 2017, with the theme "Actuarial Research at the Crossroads: Transcending Disciplines." Actuarial educators, practitioners and researchers gathered together to discuss the latest developments and to exchange ideas. In this issue of Risk Management, we are pleased to invite Dr. Wang to share a summary of his presentation at the ARC, "Modeling of Optimal Spending and Allocation on Cybersecurity."

INTRODUCTION

The rising number of cyber breaches has spurred cybersecurity spending by firms. It is estimated (e.g., Gartner, 2017)[1] that globally, the private sector invests $93 billion in 2018 to beef up their internal system's defense against cyber threats. Firms want to know the optimal level and allocation of security investment. Such questions have been extensively explored in the academic literature (e.g. Gordon and Loeb (2002);[2] (Tanaka, et. al (2005)).[3] At the 52nd Actuarial Research Conference, I presented a mathematical model for cyber breach probability as a function of security spending in protecting a firm's ICT systems, and derived optimal level of security investment as percentage of value-at-risk. This article also summarizes the first part of the mathematical model in Wang (2017).[4]

A firm's ICT system generally has an **attack surface** that is exposed to various types of cyberattacks. The attack surface of a firm's ICT system may include open ports on the web and mobile devices, computing services inside the enterprise firewall, and employees with access to sensitive information being socially engineered (see Figure 1). A firm's ICT system is vulnerable to various types of cyberattacks, including malware, DDOS, POS intrusions, phishing and social engineering, advanced persistent attacks, insider and privileged misuse of access, etc.

Firms normally have already invested in some cybersecurity measures to protect its ICT system. A positive security investment, $B>0$, is selected as the *benchmark spending* appropriate for the size of the attack surface. Any amount of security spending Z can be described by the *spending ratio*, $z = Z/B$. For security spending $Z=zB$, we denote the ICT system's cyber breach probability by $v(z)$. At benchmark spending B, we have z=1, the firm's ICT system has a cyber breach probability $v(1)$.

One can specify the following regularity conditions for the security breach probability function $v(z)$:

1. $v(0)=1$. When there is zero security spending, there is probability one of being breached.
2. $v'(z)<0$, for $z>0$. As security investment z increases, the cyber breach probability $v(z)$ decreases. In other words, every additional dollar spent yields proportionally less benefit in reduction of vulnerability. A firm ideally should invest into those tools whose return is highest. This return is the rate at which the residual breach probability reduces with incremental increase of the investment z. This rate is non-increasing if the current investment is optimal, as the best protection is acquired first. This intuitive assumption is supported empirically on cross-sectional firm data (e.g., Tanaka et al, 2005).

Wang (2017) considered several classes of cyber breach probability function.

a. The Exponential Power Class:

$$v_{EP}(z) = v(1)^{z^{\alpha}}, \text{ where } \alpha > 0 \qquad \text{(eq-3)}$$

b. The Proportional Hazard (PH) Class:

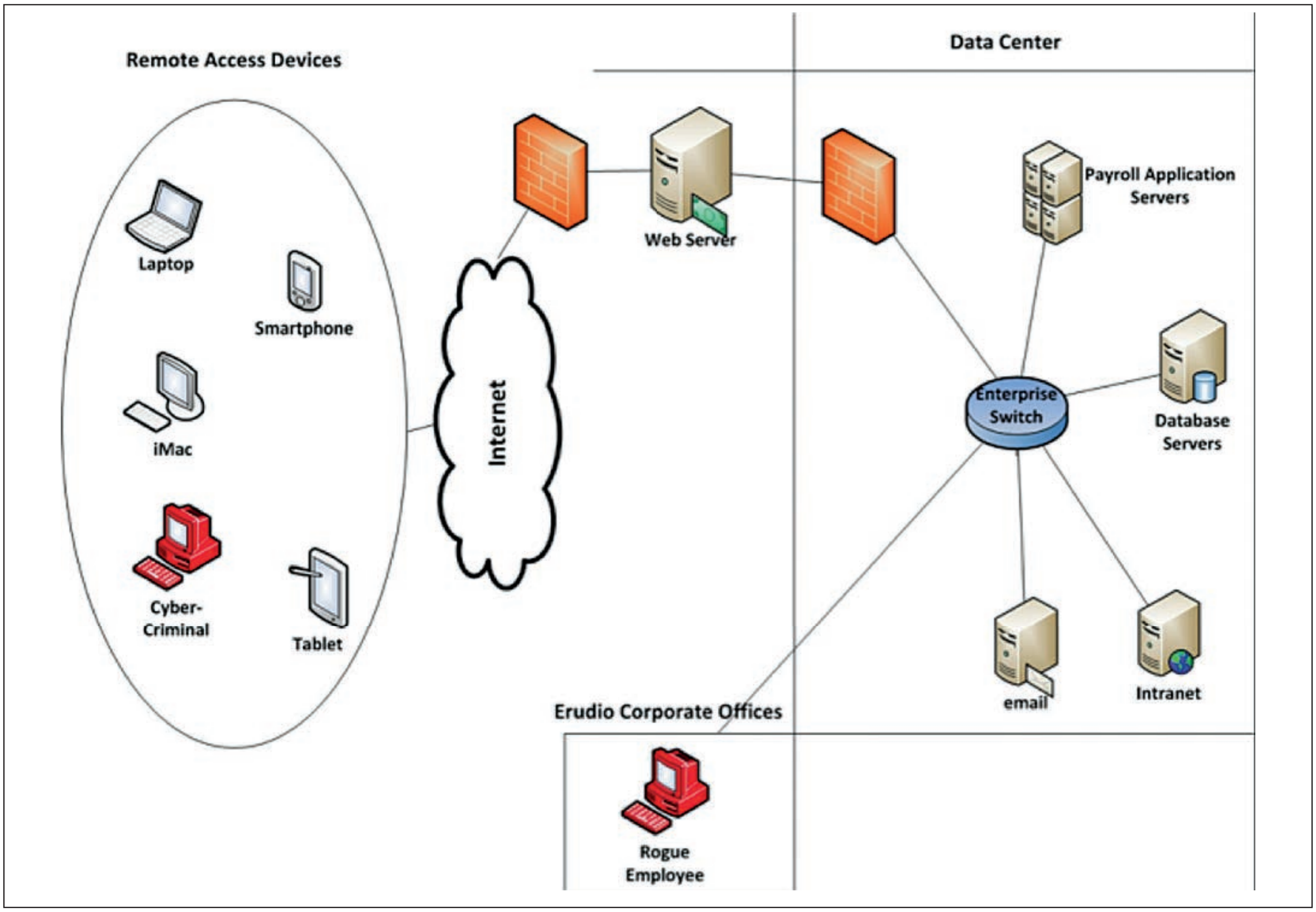
$$v_{PH}(z) = 1 - [1 - v(1)]^{z^{-\alpha}}, \text{ where } \alpha > 0 \qquad \text{(eq-4)}$$

c. The Wang Transform (WT) Class:

$$v_{WT}(z) = \Phi[\Phi^{-1}(v(1)) - \alpha \cdot \ln(z)] \qquad \text{(eq-5)}$$

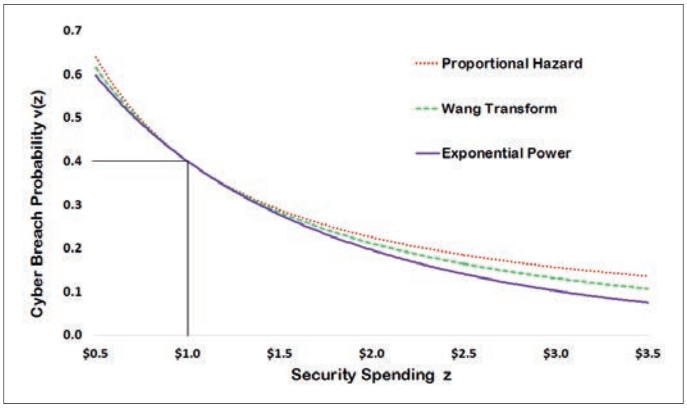
where $\alpha > 0$ and Φ is the cumulative standard normal distribution (see Wang, 2000).[5]

Figure 1
An Illustration of an Attack Surface



Source: *http://www.infosecinstitute.com*

Figure 2
Comparison of Cyber Breach Probability Functions



The cyber breach probability function $v(z)$ is said to have an **invariance** property if the same functional form is preserved under a change of benchmark: $\tilde{B}=\tau\cdot B$, for all $\tau>0$. One can verify that the Exponential Power, the Proportional Hazard, and the Wang Transform classes of cyber breach probability functions all have invariance property, with the functional form and the parameter α remains the same for different choices of the benchmark B.

OPTIMAL LEVEL OF SECURITY SPENDING

Consider a firm's ICT system. Let R represent the potential value-at-risk, or monetary losses and expenses given the occurrence of data breach. Corresponding to the security spending $Z=z\cdot B$, the firm has a cyber breach probability, $v(z)$, and an annual loss expectancy (ALE) of $v(z)\cdot R$. The total cyber cost to the firm is the sum of security spending Z and annual loss expectancy:

$$\text{Cost}(z) = z \cdot B + v(z) \cdot R$$

The optimal spending ratio z^* is defined such that the firm's cyber cost is minimized at security spending $Z^* = z^* \cdot B$. The optimal level of security spending $Z^* = z^* \cdot B$ satisfies the equation:

$$-v'(z^*) = B/R$$

In the special case of the Exponential Power Class with $\alpha = 1$, the optimal spending ratio has a closed-form formula:

$$z^* = \frac{\ln(R) - \ln(B) + \ln(-\ln v(1))}{-\ln v(1)}$$

Remark: The derivative $-v'(1)$ indicates the *effectiveness* of incremental spending in reducing the vulnerability, at the benchmark spending B.

One can verify that the optimal security investment $Z^* = z^* \cdot B$ has the following upper bounds:

1. For the Exponential Power Class: $Z^* \leq \frac{\alpha}{e} \cdot R$
2. For the Proportional Hazard Class: $Z^* \leq \frac{\alpha}{e} \cdot R$
3. For the Wang Transform Class: $Z^* \leq \frac{\alpha}{\sqrt{2\pi}} \cdot R$

OPTIMAL SECURITY INVESTMENT ALLOCATION TO ADDRESS MULTIPLE AREAS OF VULNERABILITY

Consider that an ICT system which has multiple areas of vulnerability, and cyber breach occurs when a hacker successfully exploits any one area of vulnerability (see Figure 3). We choose the number of areas of vulnerability to be three, although the analysis holds for any number of areas of vulnerability. For each area j of vulnerability ($j = 1, 2, 3$), the benchmark spending is B_j, with a corresponding cyber breach probability, $v_j(1)$. Assume that the organization's security spending $\boldsymbol{Z}$ is allocated to address each area of vulnerability:

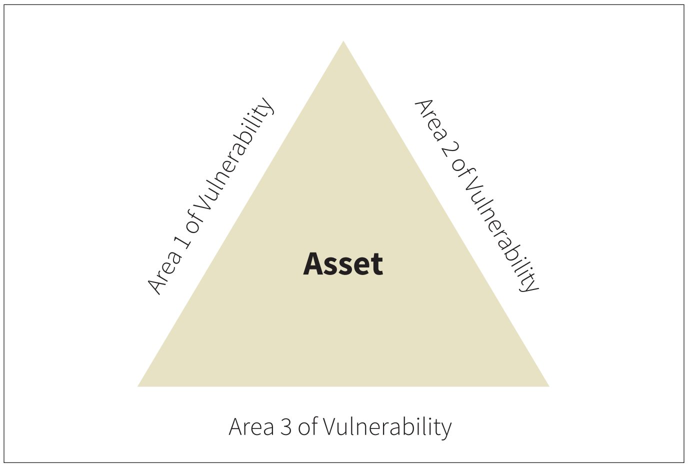
$$\boldsymbol{Z}^* = z_1 \cdot B_1 + z_2 \cdot B_2 + z_3 \cdot B_3$$

We have a competing risk model:

$$v(z) = 1 - (1 - v_1(z_1)) \cdot (1 - v_2(z_2)) \cdot (1 - v_3(z_3))$$

Our model and analysis highlight the importance of security spending to cover the full spectrum of areas of vulnerability; neglecting one area of vulnerability can render the security investment ineffective and wasteful. Moreover, economic value can be gained by differential treatment of the high-value data assets. Firms should give priority protection of their crown-jewel assets (say, by reducing unnecessary connection points and/or by imposing multi-factor authentication).

Figure 3
Parallel Routes or Multiple Areas Vulnerability



The benchmark model in this paper has practical implications. It is advisable for firms to anchor their security spending to some benchmark, and empirically track effectiveness of security spending in reducing vulnerability. For firms, assessing the vulnerability of tis ICT system would require IT expertise and knowledge; identifying the key data assets would require knowledge of the firm's business model. Thus, there is a need for coordination between IT experts and enterprise risk managers. ■

Shaun S. Wang, FCAS, CERA, Ph.D., is professor and director, Insurance Risk and Finance Research Centre, Nanyang Business School, Nanyang Technological University, Singapore. He can be reached at *shaun.wang@ntu.edu.sg*

ENDNOTES

[1] Gartner, 2017. Gartner Predicts Information Security Spending To Reach $93 Billion In 2018, Reported by Forbes. *https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#22a572db3e7f*

[2] Gordon, Lawrence A. and Martin P. Loeb, 2002. "The Economics of Cybersecurity Investment". ACM Transactions on Information System Security, 5, 438–457.

[3] Tanaka, H., Matsuura, K., Sudoh, O. 2005. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy* 24 (2005) 37–59

[4] Wang, Shaun, 2017. Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain (November 3, 2017). Available at SSRN: *https://ssrn.com/abstract=3064533*

[5] Wang, Shaun, 2000. "A Class of Distortion Operators for Pricing Financial and Insurance Risks." *Journal of Risk and Insurance*, 67 (2000 March): 15–36.