SINGAPORE ACTUARIAL SOCIETY

# Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain

**Dr. Shaun Wang, FCAS, CERA**

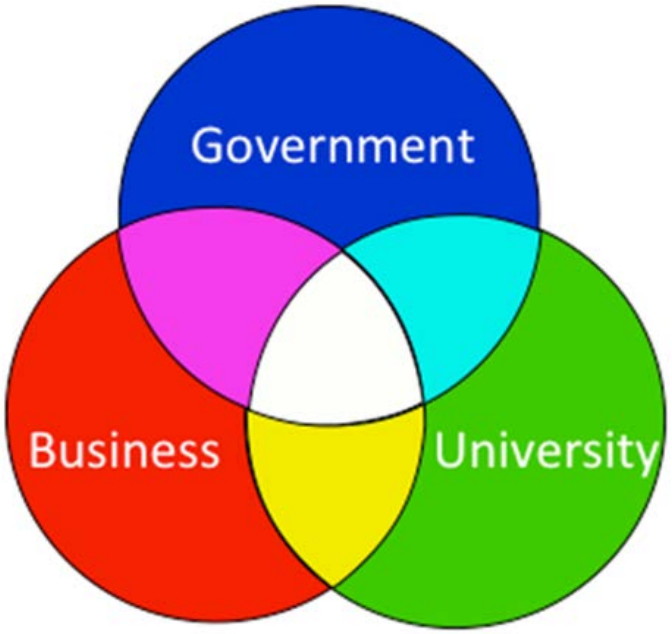
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE | Nanyang Business School

# Cyber Risk Management Project

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE | Nanyang Business School

**Government-University-Industry Collaboration**

- Monetary Authority of Singapore
- Cyber Security Agency
- Nanyang Technological University
- SCOR； Aon； MSIG； Lloyd's； TransRe；
- Geneva Association; Verizon

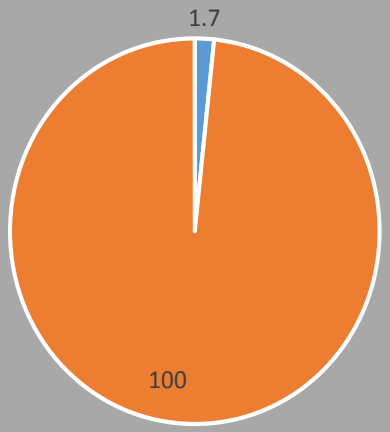



Launched in 2016

# Cybercrime Damage >> Security Spending >> Cyber Insurance

- Global cybercrime loss = $3 trillion in 2015.
- Cybersecurity budget =$100 billion per annum
- 2015 global standalone cyber insurance premium = $1.7 billion (ref. Aon)
- At the firm level,
  - What is the benchmark security budget?
  - How effective is the security spending?

# Cyber Crime Damage = Square Shaded Area



# 2017 Data Breach at Equifax


- Data breach occurred between May-July 2017, hackers exploited a flaw in Apache Struts
- A patch was released on March 7, yet Equifax failed to apply security updates
- This is surprising given that Equifax and its insurance partners trumpeted their “cyber expertise”
- Share price dropped 33% immediately following
- CEO replaced; CIO and CISO stepped down
- Equifax insurance claim $125 million, only a fraction of actual cost ($1-$4 billion)

# Gold Rush to Cybersecurity Tools

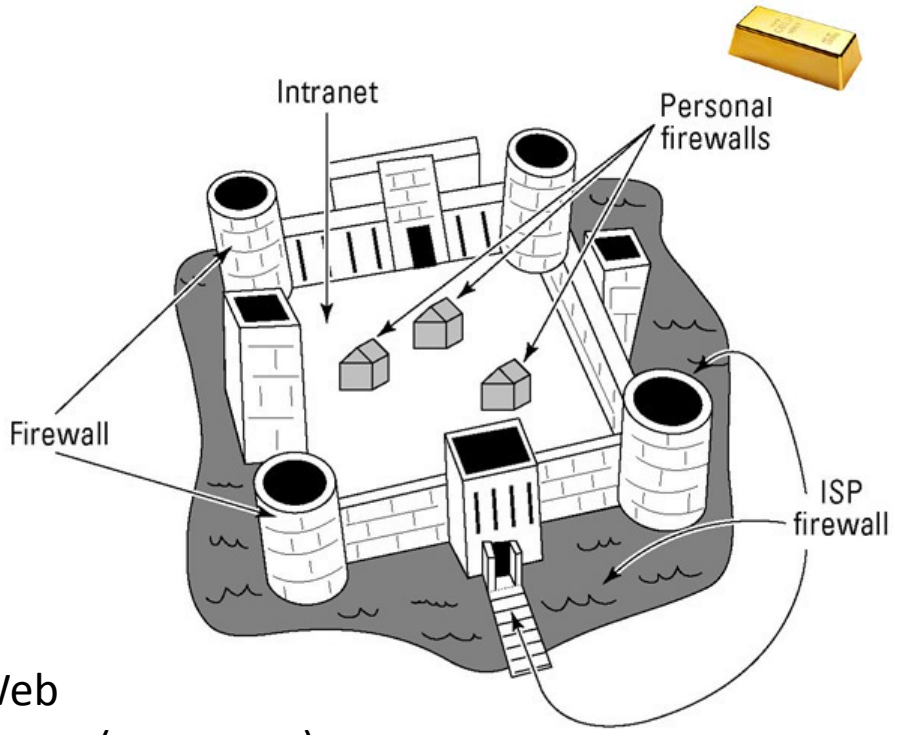
- In April 2017, the RSA Cybersecurity Conference in San Francisco attracted about 43,000 attendees with many exhibitors of new products and software (driven by venture capital investments).
- But organizations face *different* kind of challenges.
- To prevent large gaps between R&D investment and consumption by the business community, we need first map out business problems and then develop solutions.

# Conventional Loss Model


- The number of cyber threats *n*.
- The **vulnerability** or probability *v* of data breach per cyber threat.
- The i**mpact** or monetary loss, $\lambda$, in the event of data breach.
- The remaining **annual loss expectancy**

$$loss_{firm} = n \cdot v \cdot \lambda$$

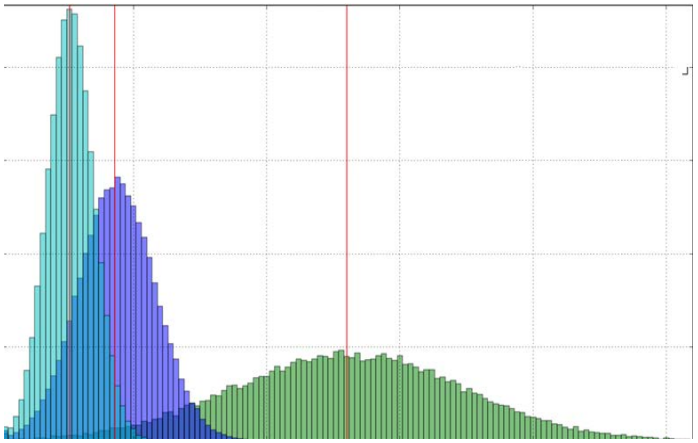
# Illustration: Threats, Vulnerability and Impact




Fast-growing Dark Web
Malware & Ransomware (arms race)

# Traditional Insurance Risk

- Randomness
  - Law of Large Numbers
- Diversify through risk transfer

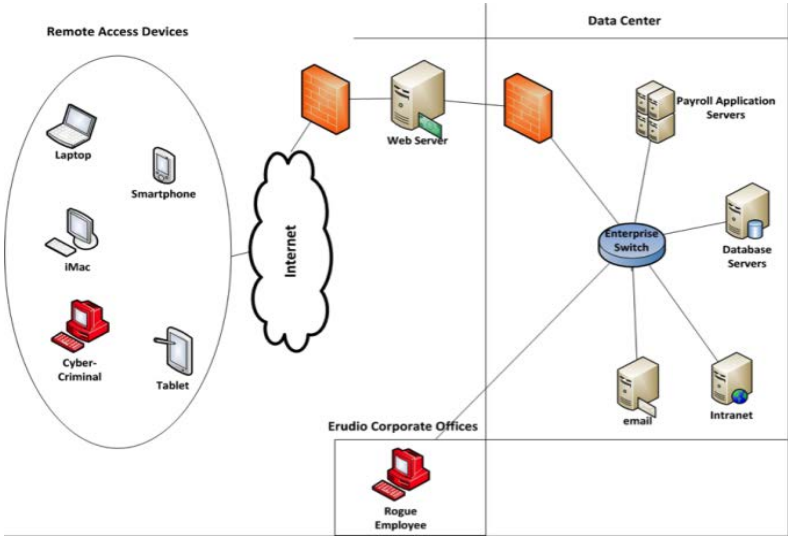


# Cyber Risk

- Human Factors
  - Hackers, fishing
- Strengthen defense reduces risk

# Attack surface

# "knowledge set"

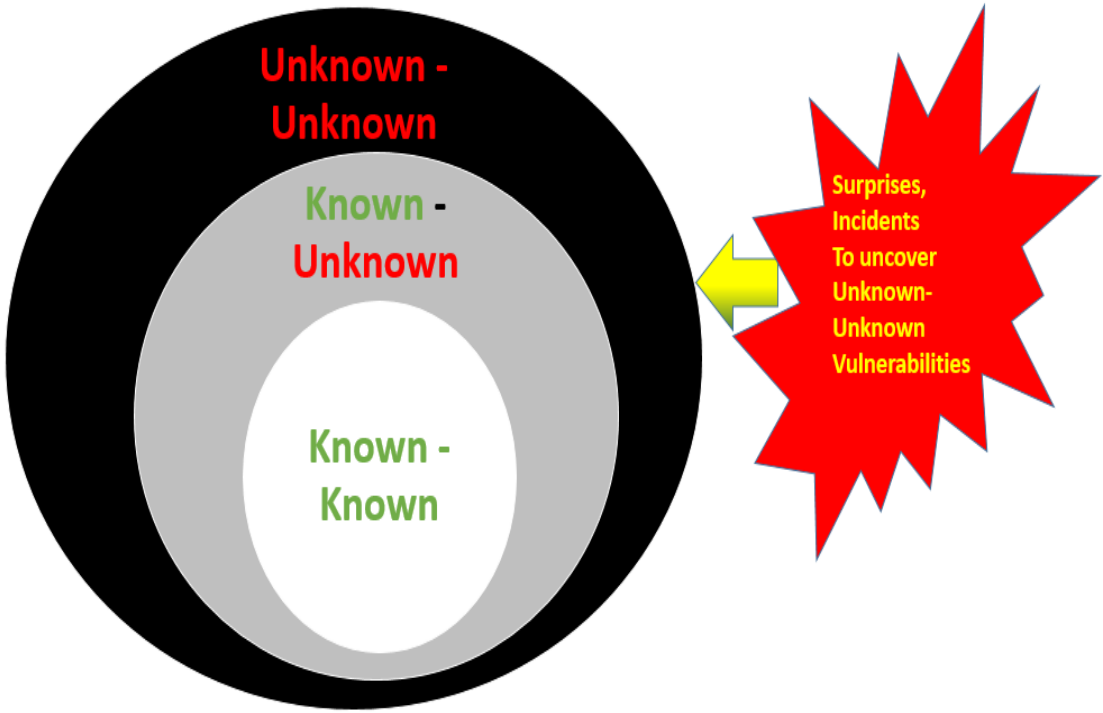



**Knowledge Set is a *relative* concept:**

1) WHO
2) What

- *actually knows*
- *should know but not know*
- *Unknown unknown*

1) How



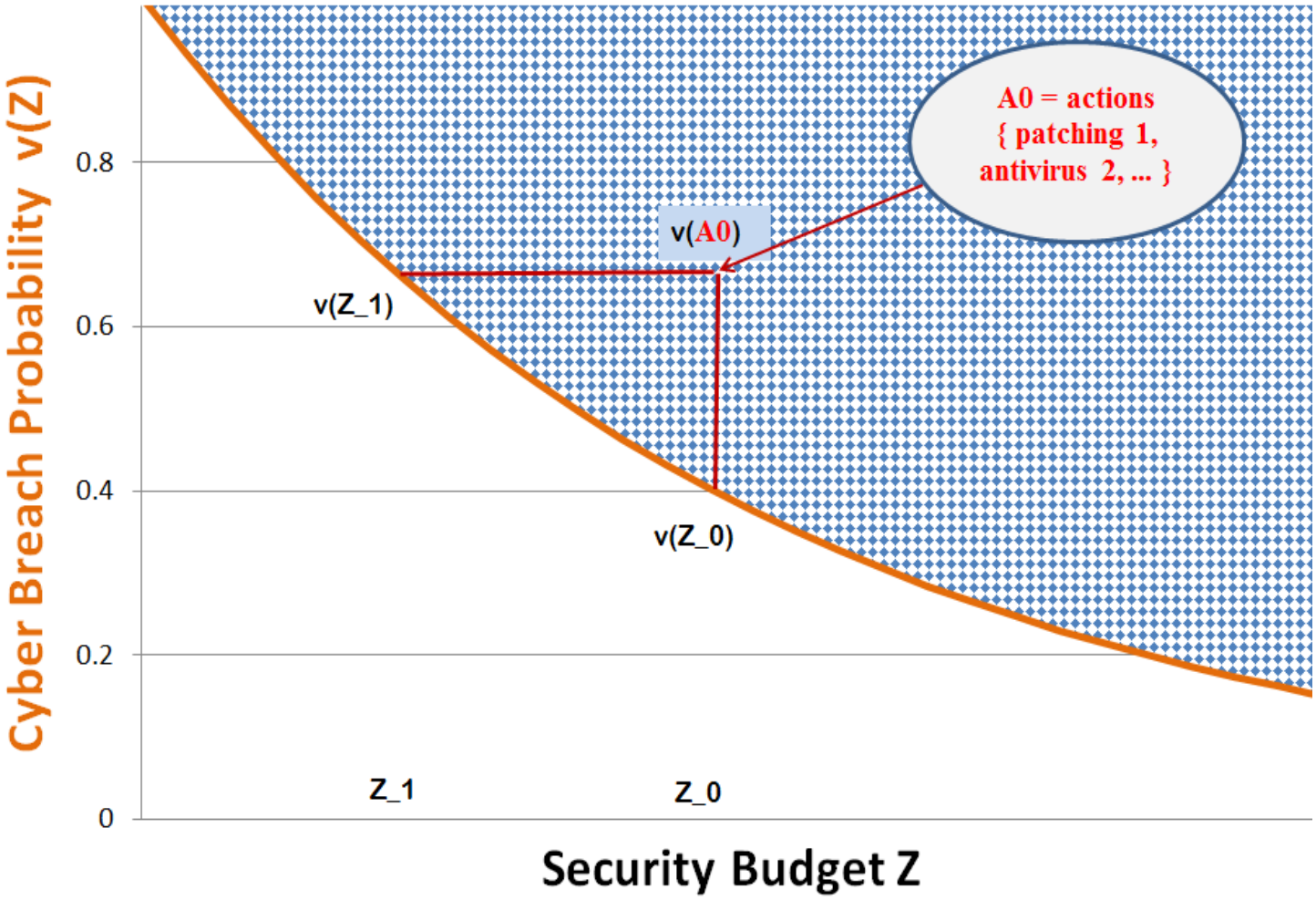
# Knowledge Set & Cyber Breach Probability

- Given knowledge set Ω, for a given budget $z$, the firm may select any possible mitigating action $A \in \Omega$ within budget $z(A) \leq z$.
- Define

$$v_{\Omega}(z) = \min_{A \in \Omega:\, z(A) \leq z} v(A)$$

  - $v(0)$=1. If zero security investment, the firm would have a probability one of being breached.
  - $v'(z)$<0, for $z$>0.

# Security Spend Production Frontier



# Benchmark Spending & Risk Reduction Equation

- **benchmark** security budget $z_0$=*f*(revenue)
- spend ratio $^{z}/_{z_0}$

1) Exponential Power

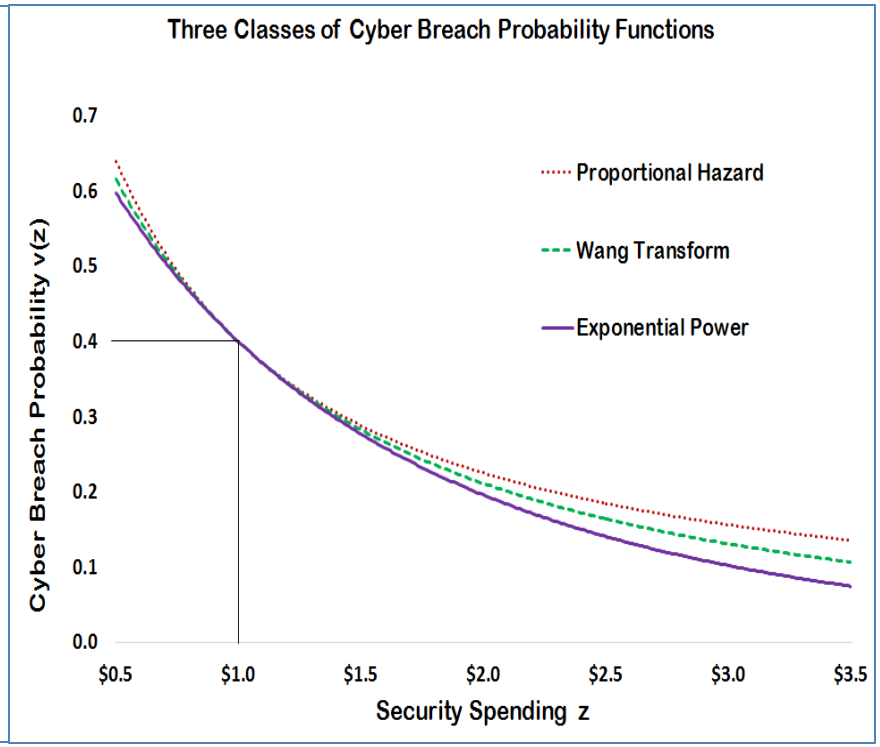
$$v(z) = v(z_0)^{\left(\frac{z}{z_0}\right)^{\alpha}}$$

2) Proportional Hazard

$$v(z) = 1 - [1 - v(z_0)]^{\left(\frac{z}{z_0}\right)^{-\alpha}}$$

3) Wang Transform

$$v(z) = \left[\Phi^{-1}(v(z_0)) - \alpha \cdot \ln\left(\frac{z}{z_0}\right)\right]$$



# Optimal Security Spending

- A firm's data asset value *R*, optimal spending $z^*$ minimizes

$$\text{Total Cost: } \{\ \ z + v(z) \cdot R\ \}$$

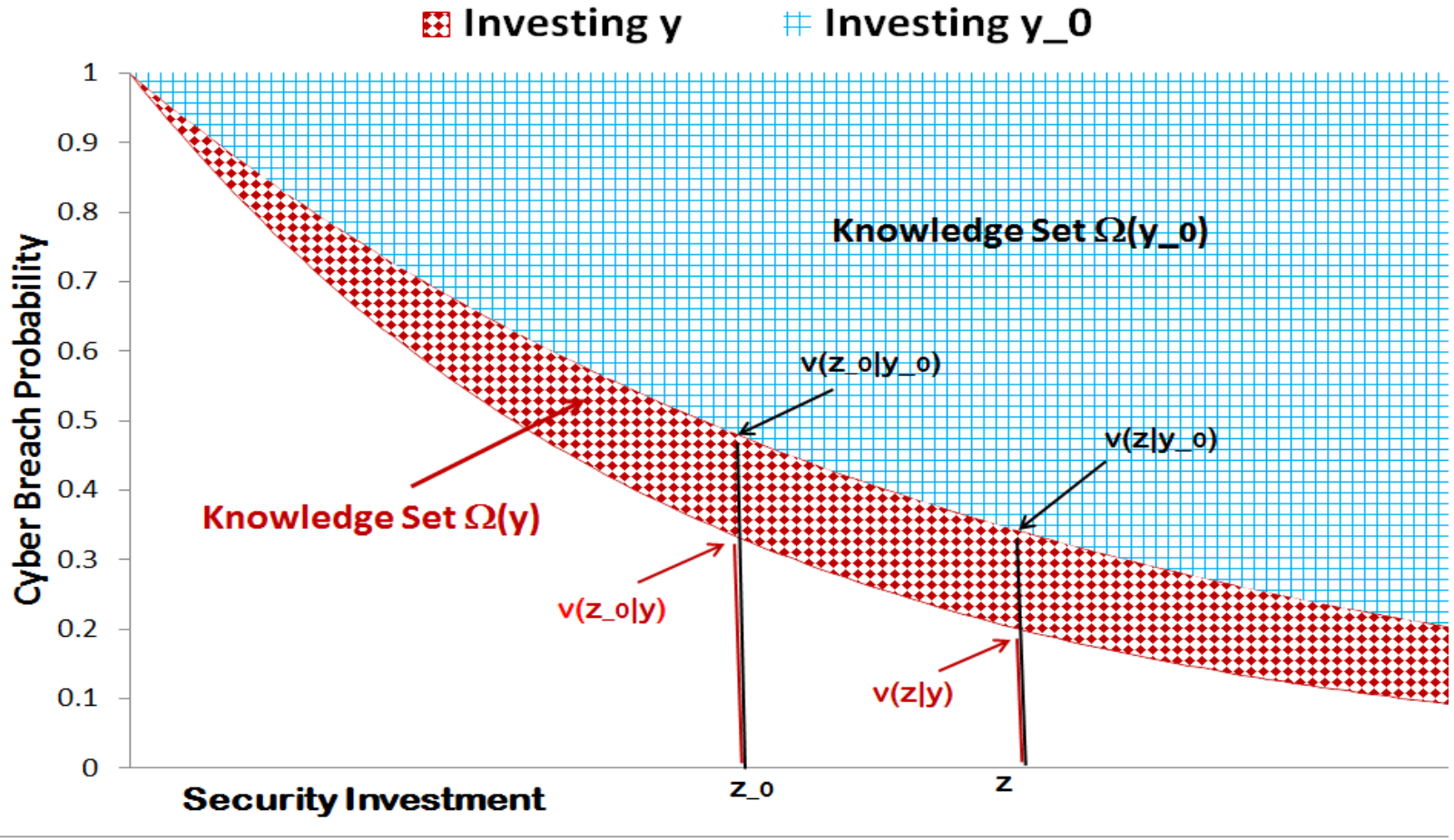
- For Exponential Power and PH curves, the optimal spending

$z^* \leq \frac{\alpha}{e} \cdot R$ …… 1/e rule [Gordon-Loeb model]

- For Wang Transform curve, the optimal spending

$z^* \leq \frac{\alpha}{\sqrt{2\pi}} \cdot R$ …… 1/SQRT(2$\pi$) rule

# Invest: (1) “y” in data/information, (2) “z” in defense/response



# Two Types of Investment

*1: Invest y in data, information and expertise*

$$v(\bullet|y) = (v(\bullet|y_0))^{(\frac{y}{y_0})^{\beta}}$$

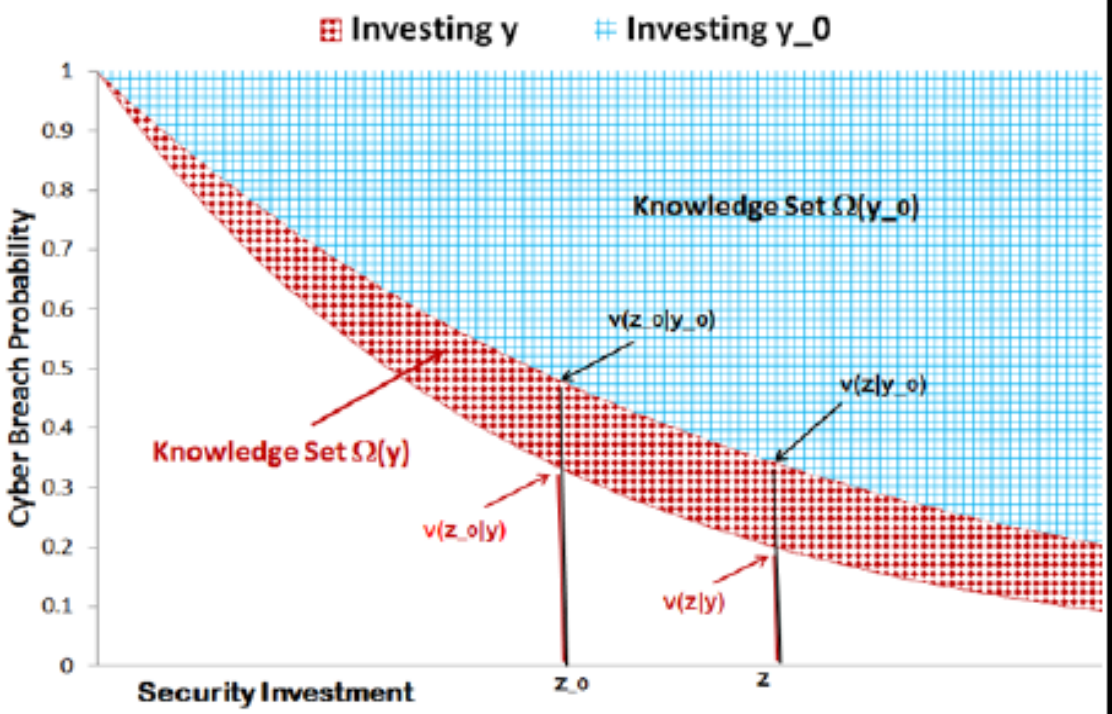
*2: Invest z in defense/detection tools*

$$v\,(|\bullet) = (v(z_0|\bullet))^{\left(\frac{z}{z_0}\right)^{\alpha}}$$

*3: Combined effect:*

$$v(z|y)$$

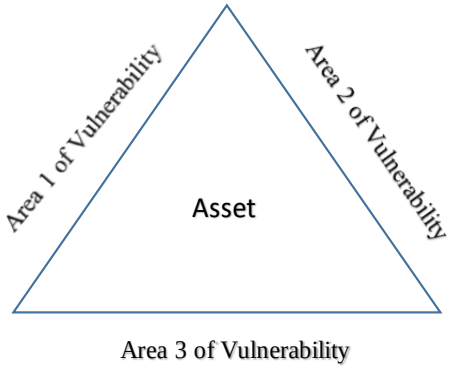
$$= (v(z_0|y_0))^{(\frac{y}{y_0})^{\beta}\cdot(\frac{z}{z_0})^{\alpha}}$$

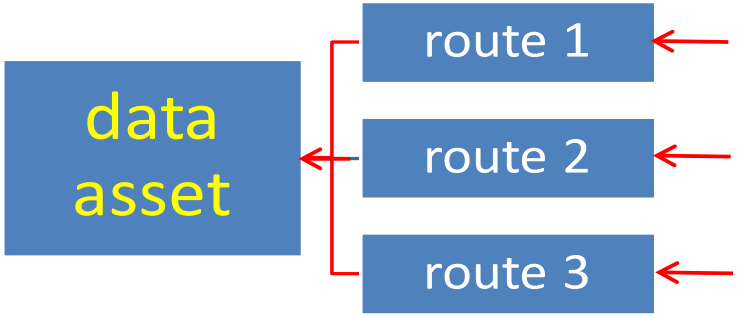



**Theorem:** Optimal security investment allocation:

$$y^*/z^* = \beta/\alpha$$

# Multiple Areas of Vulnerability



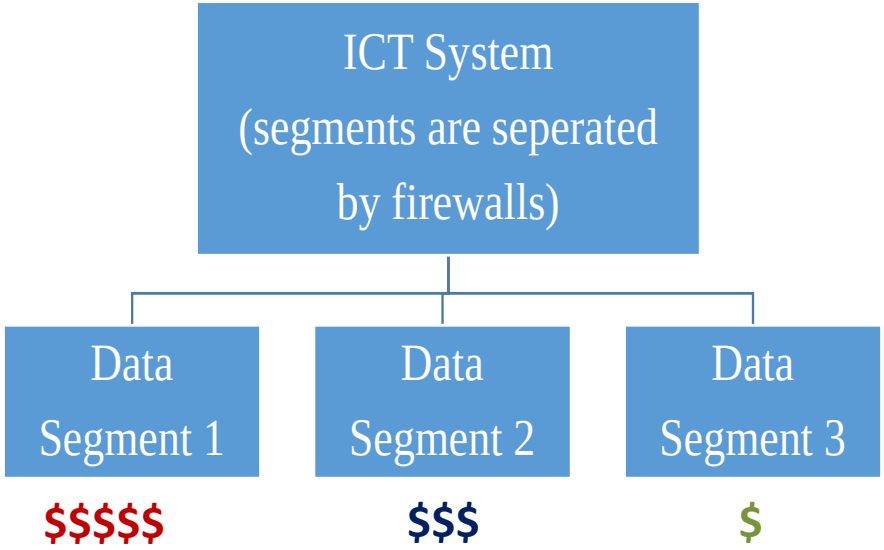




$$1 - v(Z) = \left(1 - v(z_1)\right) \cdot \left(1 - v(z_2)\right) \cdot \left(1 - v(z_3)\right)$$

- Need to secure the *full spectrum* of areas of vulnerability
- Neglecting one area of vulnerability can render the overall security investment ineffective or wasteful

# Data Segmentation & Multiple Checkpoints

$$v(Z) = v_1(z_1) \cdot v_2(z_2)$$


- Multi-factor authentication very effective
- Need protect key ($$$$$) data assets with extra security measures

# In Search for Cost-Effective Ways of Reducing Known Unknown

- SINGAPORE (12 Dec 2017)— In a first for a government agency here, 300 "white-hat" hackers will be invited to put the Ministry of Defence's public-facing systems to the test, in order to expose vulnerabilities.
- *"The rewards will hinge on the number and quality of the vulnerabilities exposed, and are expected to cost significantly less than a commercial cyber-security vulnerability-assessment programme, which can cost up to S$1 million. In contrast, the new bug-bounty initiative is estimated to cost around S$100,000, said Mr Koh, who also heads the CSA."*

*Accessed from https://www.gov.sg/news/content/today-online---mindef-invites-hackers-to-test-public-facing-systems-for-vulnerabilities*

# RAND studies of 100 cyber insurance policies in 3 States (NY, NJ, CA)

- The first and most important firm characteristic used to compute insurance premiums was the firms asset value (or revenue) base rate, rather than specific technology or governance controls,
- Premium estimates for policies that cater to small business are very simple,
- While some carriers have sophisticated algorithms for premium estimates, many policies used generic security risk categories (high med low)

# Cyber Insurance Rating Model

(ref. Romannosky, 2017)

CyberOne policy, developed by Insurance Services Organization (ISO), is used by many smaller insurance companies and offers first and third party premiums as shown in Table 5.

Table 5: Simple Rate Development

| Coverage | Frequency | Severity | Expected Loss (Lost Cost) | Profit Load | Premium |
|---|---|---|---|---|---|
| Computer Attack | 0.20% | $49,800 | $99.60 | 35% | $153 |
| Network Security Liability | 0.17% | $86,100 | $147.23 | 35% | $227 |

Table 9 : Limits Factor

| Limits | Factor |
|---|---|
| $500,000 | 0.809 |
| $1,000,000 | 1.000 |
| $2,000,000 | 1.132 |
| $3,000,000 | 1.245 |
| $4,000,000 | 1.371 |
| $5,000,000 | 1.405 |

# So why didn't Cyber Insurance **fully** utilize "Cyber Risk Assessment"?

- Due to Knowledge Gap of the attack surface – dynamically changing
- Ambiguity of insurance coverage issues
- With lacking of *scale* of cyber insurance, the cost of information out-weights underwriting edge

# Email Attack on Vendor Set Up Breach at Target

"The breach at **Target Corp.** that exposed credit card and personal data on more than 110 million consumers appears to

- have begun with a malware-laced email phishing attack sent to employees at a **Heating, ventilation, and air conditioning** (**HVAC**) **firm** that did business with the nationwide retailer, ..."



Accessed from https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

# Supply-chain Propagation Model

- Let $\theta_{i,j}$ be the likelihood that a cyber breach into firm *i* will export to firm *j*
- $\theta_{i,j} \neq \theta_{j,i}$ (non-symmetric)
- Matrix of propagation coefficients:

$$\begin{pmatrix} 1 & \theta_{1,2} & \dots & \theta_{1,m} \\ \theta_{2,1} & 1 & \dots & \theta_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{m,1} & \theta_{m,2} & \dots & 1 \end{pmatrix}$$

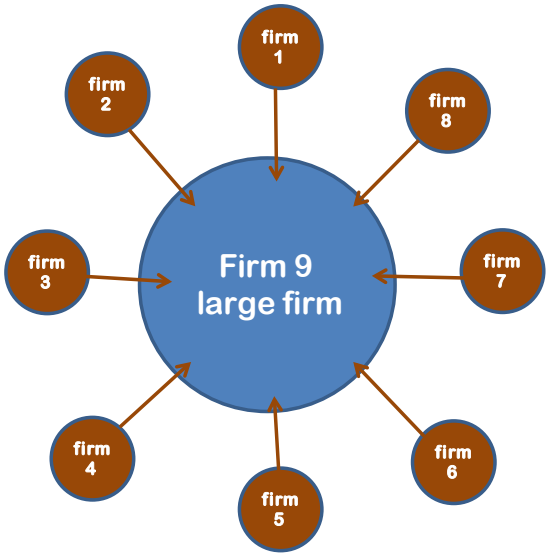
# Cyber Breach Probability in a Supply-Chain

- Let $Z = (z_1, z_2, \ldots, z_m)$ be security investments by the *m* firms.
- firm *j* faces a combined cyber breach probability:

$$\tilde{v}_j(Z) = \sum_{i=1}^{m} \theta_{i,j} \cdot v_i(z_i)$$

- firm *j*'s contributes to the eco-system's expected cyber loss:

$$v_j(z_j) \cdot \left(\sum_{i=1}^{m} \theta_{j,i} \cdot R_i\right)$$



# Optimal Security Spend for the eco-system

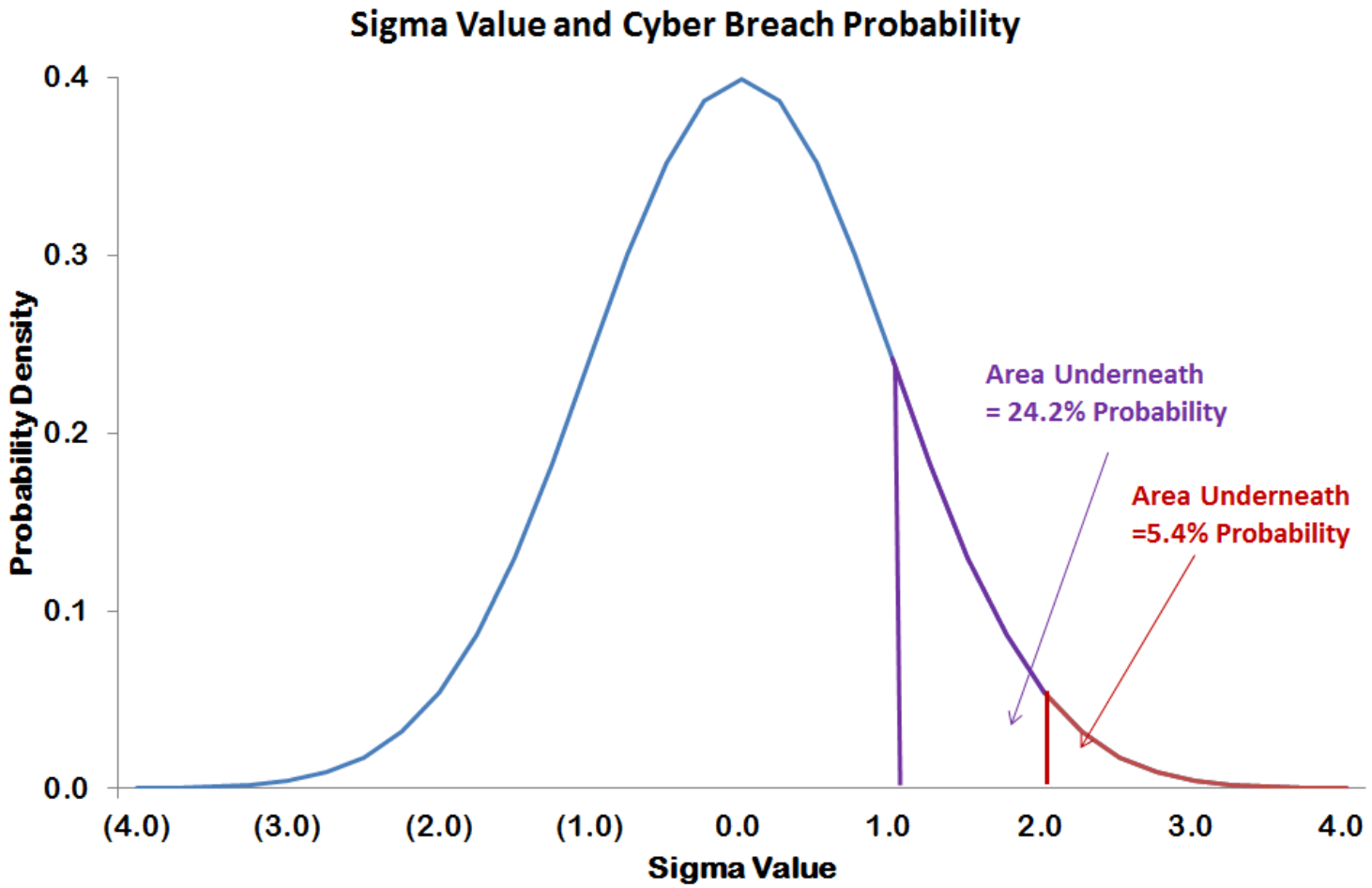
| | Standalone spending $z_j^*$ | Eco-system Spending $\tilde{z}_j^*$ | $\frac{\tilde{z}_j^*}{z_j^*} - 1$ |
|---|---|---|---|
| **Small firm** | $ 1.31 | $ 2.22 | +70% |
| **Large firm** | $10.09 | $11.43 | +13% |

1) Optimal spend by small firm need to increase +70% in a supply-chain setting vs standalone (as compared to +13% for large firm)
2) However, small firms have no incentives to voluntarily do that! **This is the problem!**

# **Knowledge Gap** about Security Level of 3rd Party Vendors

1) Large firms invest $$$$$ to their own cyber security, but are vulnerable to the **lack of knowledge** for the security level of their suppliers
2) To overcome such **knowledge gap**, large firms may require suppliers to provide cyber security rating
3) But **how good (reliable)** is the cybersecurity rating? [similarly how good are the security audits?]

# Cyber Breach Probability in Sigmas

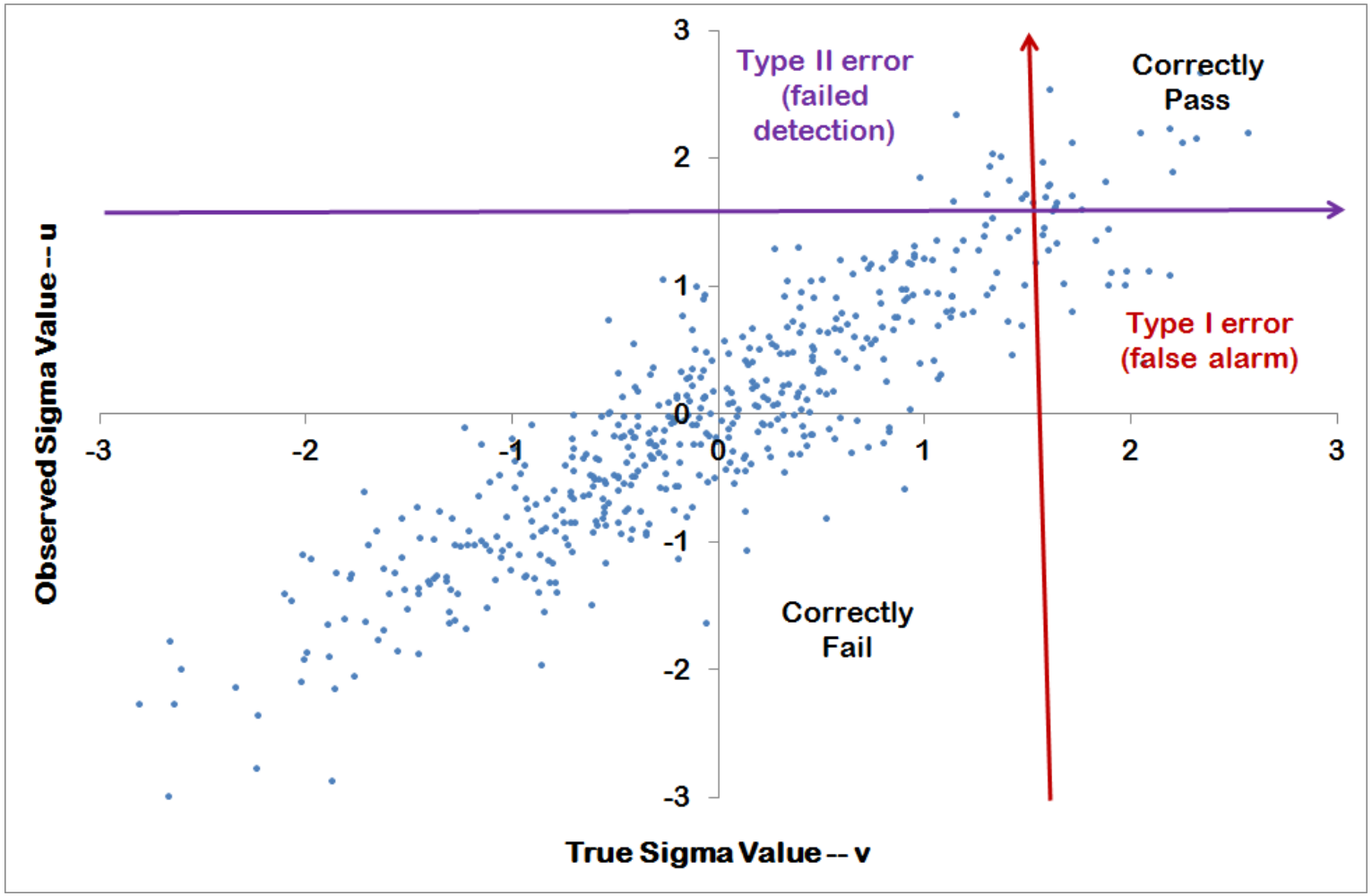


# Gaussian Copula model for security level rating

- Assume *estimated* security level *u* and the *true* security level *v*, expressed in sigma values, $\Phi^{-1}(u)$ and $\Phi^{-1}(v)$, follow a bivariate Normal(0,1), with correlation $\rho$.
- Conditional on the true underlying sigma value $-\Phi^{-1}(v) = x_0$, the estimated sigma value $-\Phi^{-1}(u)$ has a mean of $\rho \cdot x_0$ and volatility of $\sqrt{1-\rho^2}$.

# Gaussian Copula

## {true vs observed sigmas}



# **For Supply-Chain Security:** Impose Penalty for Failing Security Rating

- Impose penalty *K* if the firm fails prescribed security rating level $x_0$ (e.g. 1.65) sigma value.
- The firm's total cost as function of security spend "z":

$$z + v(z) \cdot R + K \cdot [\Pr\{-\Phi^{-1}(u(z)) \leq x_0\}]$$

# The Actuarial Science Frontier

1. Apply the “Knowledge Set” concept in risk analysis
2. Process sources of “data” to develop consumable “Information”
3. **Will Cyber Insurance integrate “risk reduction” and “risk transfer” services?**

# For Further Details

- Wang, Shaun, Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain (November 3, 2017). SSRN: https://ssrn.com/abstract=3064533
- Wang, Shaun, Integrated Framework for Information Security Investment and Cyber Insurance (September 15, 2017). SSRN: https://ssrn.com/abstract=2918674
- Sasha Romanosky, et al (2017) Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk? WEIS 2017.
- Sasha Romanosky (2016) Examining the costs and cause of cyber incidents, Journal of Cybersecurity, Volume 2, Issue 2.

# Thank You!