CIO Decisions Conference

Hosted by DECISIONS SearchCIO.com

Security: When is Enough, Enough?

Jack Phillips
Managing Partner
The Institute for Applied Network Security

THE INSTITUTE
FOR APPLIED NETWORK SECURITY

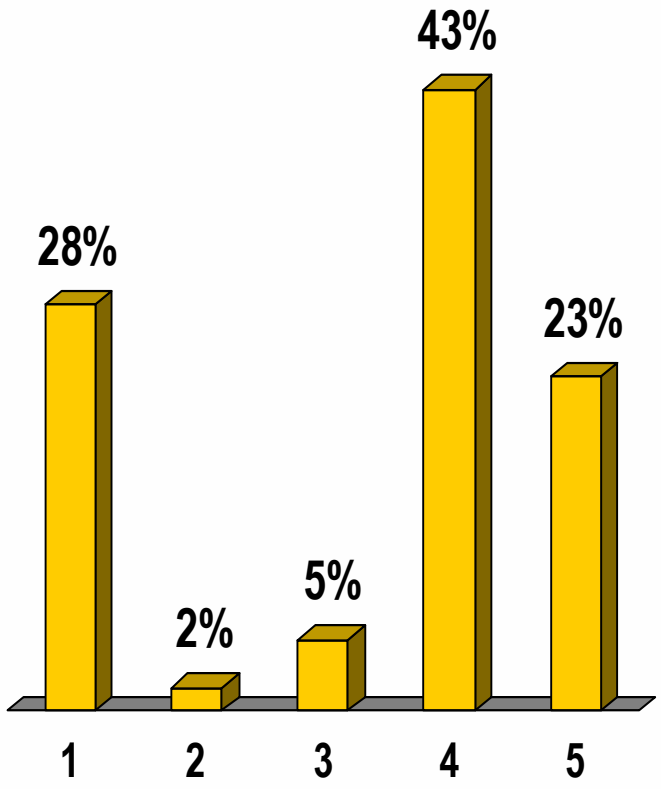
(enterprise value x 17.62%)

=

“enough security”

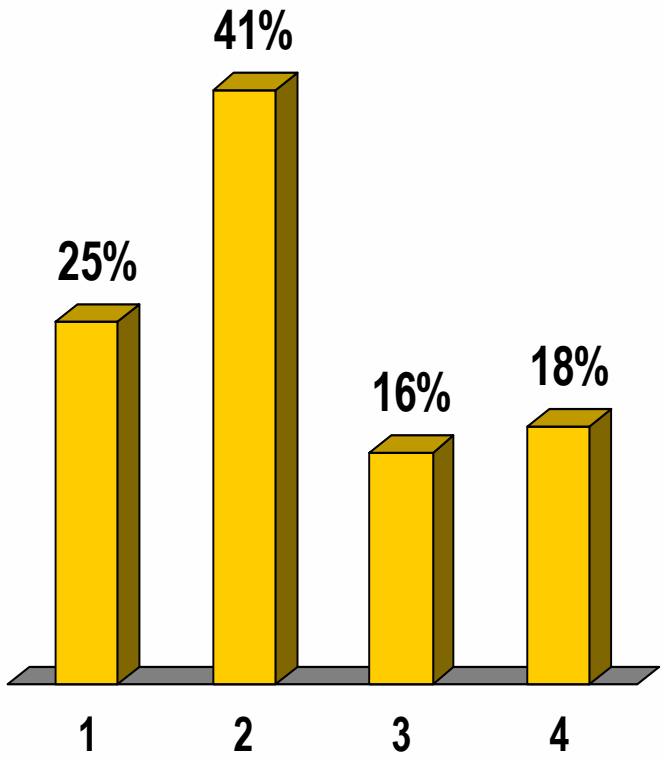
Who oversees IT Security in your organization?

1. CIO (Sr. IT Executive)
2. CISO
3. CSO
4. A designated IT professional who reports to the CIO
5. Shared among the IT staff



How secure is your organization?

1. 90%
2. 70%
3. 50%
4. <50%

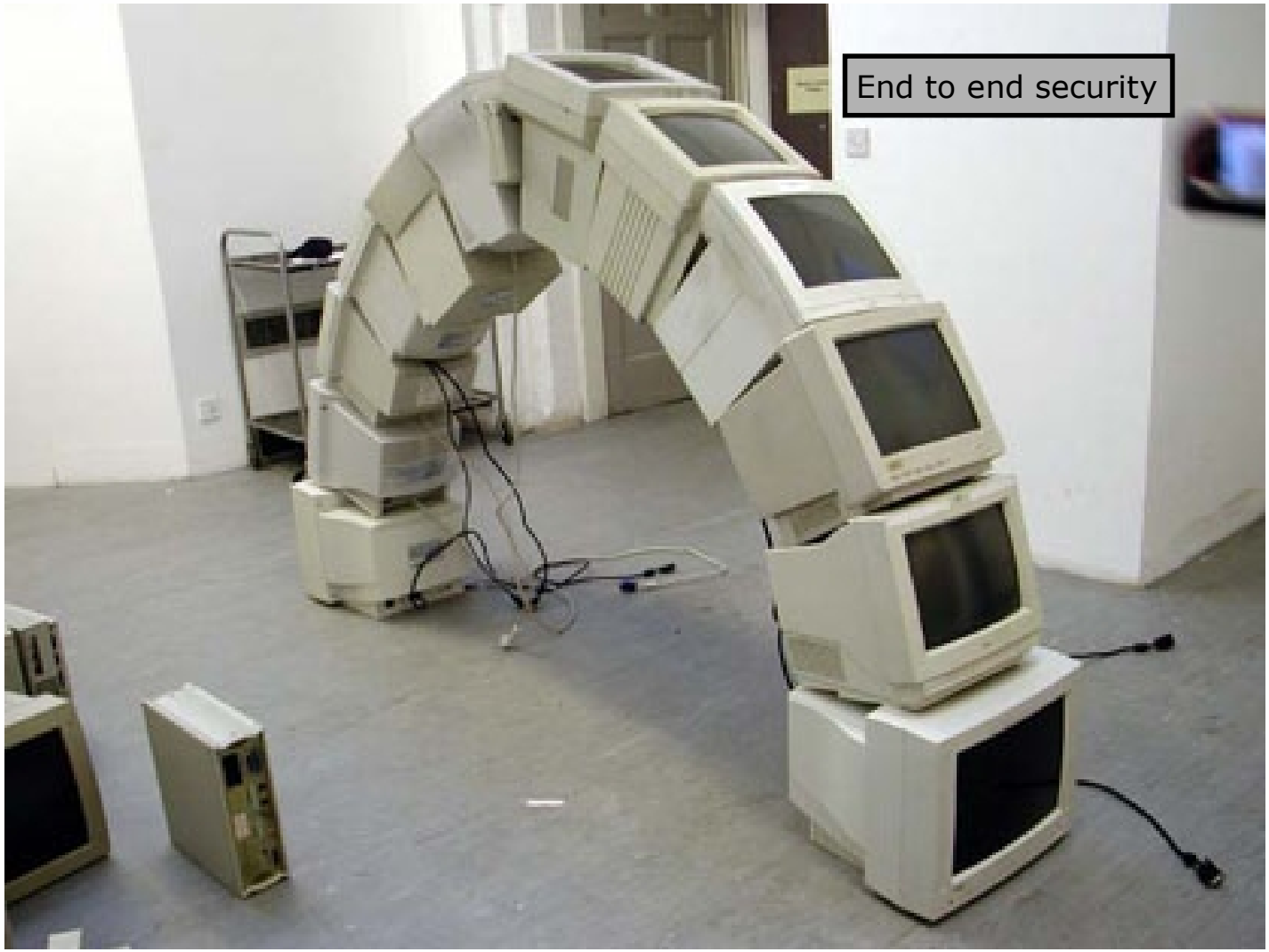


e·nough *adj.*

sufficient to meet a need or satisfy a desire; adequate; ample; suitable

One of the primary functions of executive-level management is to manage risk across the organization. An organization's security strategy and goals must be framed in the context of risk to get the attention of executive-level management. Only those risks to critical assets that threaten the accomplishment of the mission are worth attention, and then only if the organization would be significantly impacted if the risks are realized.

Carelli, The Critical Success Factor Method

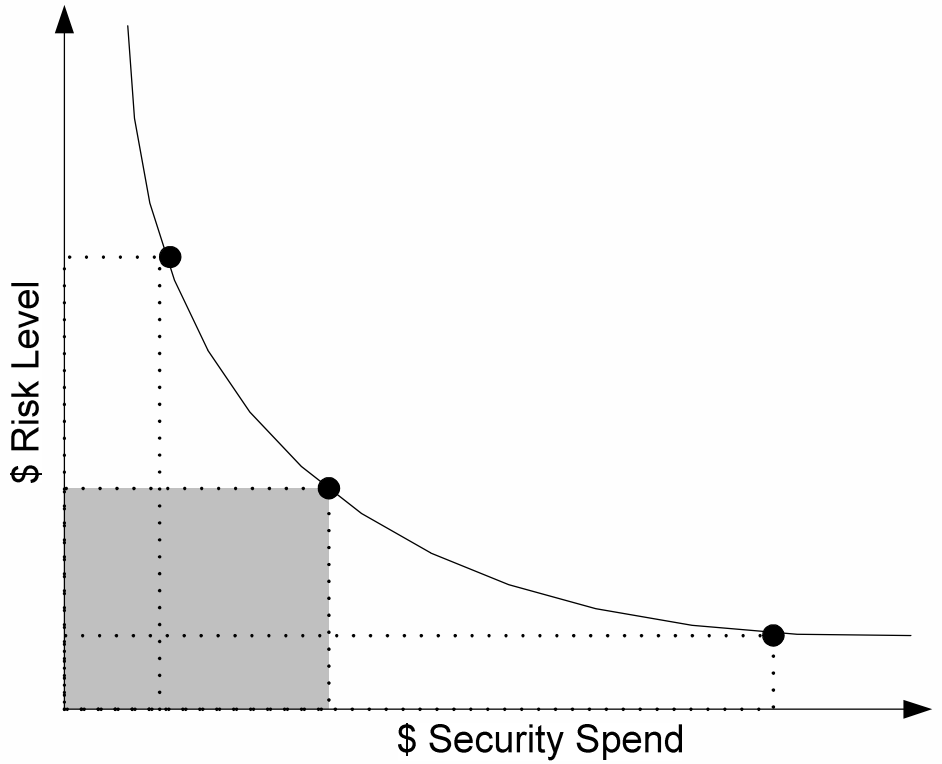

End to end security

"Some day, on the corporate balance sheet, there will be an entry which reads, 'Information'; for in most cases the information is more valuable than the hardware which processes it."

Grace Murray Hopper, USN (Ret), 1987

Equilibrium, optimality, balance

- **Strongest security posture for the lowest cost ($ spend + $ risk of loss)**
- **Security spend suffers from diminishing marginal returns (0 risk is impossible)**



Approach

1. **Start fresh**
2. **Evaluate and order critical assets**
3. **Estimate "at risk" (vulnerability) level**
4. **Determine most appropriate method for securing each asset (or class of assets)**
5. **Sum of resources spent on the methods = appropriate security posture ("enough")**

1) Start Fresh

An analysis team must apply their judgment in selecting the right areas and assets, and must ensure that their selection aligns with the business drivers of the organization. Failure to select (and validate) the right operational areas and assets can significantly diminish the value of a risk-based approach to security.

See Carelli

The hardest thing inside my organization is to get the agreement around what's important, what should be protected, and how it should be protected.

We take the "shoot first, ask questions later approach", meaning we've taken a stab at the problem and presented it to management.

It's been a starting point.

CISO, F50 Financial Institution
Mid-Atlantic Information Security Forum
February, 2006

2) Evaluate and Order Critical Assets and Success Factors

- **What are your organization's Critical Success Factors? (CSF)[1]**
- **What are the critical assets required for success?**
- **Value? (Low, High)**

Gartner, Inc.

Market Capitalization: $ 1.73B

Customers: ~10,000

Employees: 3,622 (2,174 US/1,448 Outside US)

Business: "a leading *independent* provider of research and analysis …on ...the 'IT industry'"

1)Research, 2)Consulting, 3)Events

Critical Assets: "Our success has resulted in part from proprietary methodologies, software, reusable knowledge capital and other intellectual property rights."

Security: "We recognize the value of our intellectual property in the marketplace and vigorously identify, create and protect it."

Source: Gartner 10-K, 12/31/2005

2) Evaluate and Order Critical Assets and Success Factors

- **What are your organization's Critical Success Factors? (CSF)[1]**
- **What are the critical assets required for success?**
- **Value? (Low, High)**

Asset | Criticality

- Internet traffic (customer access) | High
- Website (product) | High
- Research Database (product) | High
- Analyst Laptops (production) | High
- Brand/Service Marks | Low
- Analyst Uptime | High
- Customer Data | Low
- Extended Work Environment | Low

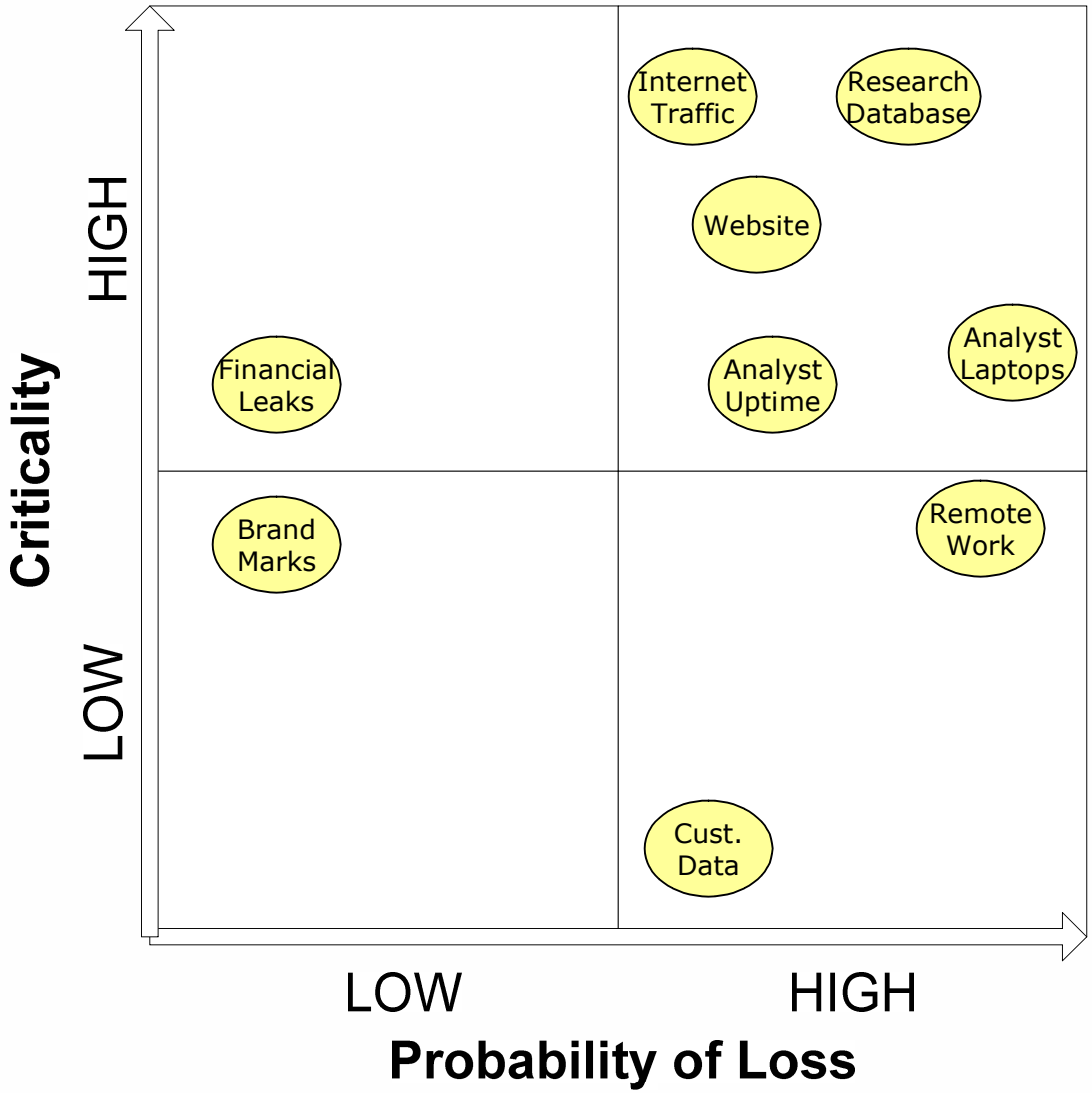
3) Estimate "at risk" (vulnerability) level

- **Consider:**
  - **External threats**
  - **Internal threats**
- **Estimate probability of loss (Low, High)**

Asset | Probability of Loss (vulnerability)

- Internet traffic (customer access) | High
- Website (product) | High
- Research Database (product) | High
- Analyst Laptops (production) | High
- Brand/Service Marks | Low
- Analyst Uptime | Low
- Customer Data | High
- Extended Work Environment | High

Criticality x Probability = Risk



Asset	Critical	Threat	Risk	Activity	Cost
Internet traffic (customer access)	High	Denial of Service (DOS)	High	Software/Hardware	$$$
Website (product)	High	Website defacement	High	Software	$$
Research Database (product)	High	Compromised Access	High	Software	$$
Analyst Laptops (production)	High	Equipment Theft	High	Training	$
Brand/Service Marks	Low	Altering, theft	Low	Acceptance	
Analyst Uptime	High	Malware (system performance)	High	Training, Software	$$
Customer Data	Low	Compromised Access	Low	Information Policies	
Extended Work Environment	Low	Wireless/VPN Compromise	High	Software	$$
Financial Info Leaks	High	Inadvertent Insider Leakage	Low	Training, Software	$

security =

***f*(hardware)+**

***f*(software)+**

***f*(policies)+**

***f*(training)+**

***f*(insurance)+ !**

Summary

- **Understand the context of your organization before you start**
- **SWAG vs. Science**
- **"Enough" comes in many flavors and shifts constantly**
- **"there can be no 100% security; determine what level of risk you can and will accept"[5]**

Parting thought

Do not stop thinking of life as an adventure.

You have no security unless you live bravely, excitingly, imaginatively.

Eleanor Roosevelt

Reference

1. Caralli, Richard et al. "The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management" (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.cert.org/archive/pdf/04tr010.pdf
2. Koetzle, L. "How Much Security is Enough?" *Forrester Research* (August, 2003).
3. Kark, K. "Are We Secure Yet?" *Forrester Research* (March, 2006).
4. Ye, Tan Shong and Hon, Loke Wing "How Much Security is Enough?" *CIO Asia* (March, 2005). http://www.cio-asia.com/ShowPage.aspx?pagetype=2&articleid=278&pubid=5&issueid=25
5. Sem, R. "Best Management Practices: How Much Security is Enough?" SEM Security Management. http://www.environews.com/BMP/security.htm