Enterprise Security Architecture

IASA Speaker: **Alvin Tan**

Definition

- Compliant to International Organization for Standardization (ISO) Standard 17799

- Necessary requirements for people, processes, and technologies

Security Strategy Questions

Security Strategy Questions

- What needs to be **PROTECTED?**
- **WHY** does it need to be protected?
- **What happens** if it is not protected?
- What potential adverse conditions and consequences need to be prevented? At what COST?
- **How much disruption** can we stand before we take action?
- How do we determine and effectively manage residual risk (the risk remaining after mitigation actions are taken)?

How much Security is Enough?

How much Security is Enough?

Characteristics to Consider

- **Organization**
- **Market Sector**

Defining Adequate Security

- **Eg.** *The condition where the protection strategies for an organization's critical assets and business processes are commensurate with the organization's risk appetite and risk tolerances.*

How much Security is Enough?

Determining Adequate Security

- What are the critical assets and business processes that support achieving your organizational goals?

- What is the organization's risk tolerances and risk appetite, in general and with respect to these assets and processes?

How much Security is Enough?

Determining Adequate Security

- Under what conditions and with what likelihood are assets and processes at risk?
- What are the possible adverse consequences if a risk is realized?
- Do these risks fit within Your risk appetite and risk tolerances?

How much Security is Enough?

Determining Adequate Security

- In the cases where risks are beyond these thresholds, what actions do you need to take to mitigate and with what **priority?**
- Are you making conscious decisions to accept levels of risk exposure and then effectively managing residual risk?
- Have you considered mechanisms for sharing potential risk impact (for example, through insurance or with third parties)?

How much Security is Enough?

Determining Adequate Security

- For those risks you are unwilling or unable to accept, what **protection strategies** do you need to put in place?

- **WHAT** is the cost/benefit or return on investment of deploying these strategies?

How much Security is Enough?

Determining Adequate Security

- How well are YOU managing YOUR security state today?
- How well will YOU manage YOUR security state 30 days, 6 months, and a year from now?
- Are YOU updating YOUR understanding and definition of our security state as part of normal planning and review processes?

Protection strategies

Protection strategies

- Principles enacted by **policies** and procedures that state these requirements and risk tolerances for this asset
- Clear assignment of roles and responsibilities and periodic **training** for staff and managers
- Periodic training for staff having access to this asset; & immediate **removal** of access and authorization.

Protection strategies

- Review all **NEW** and upgraded technologies occurs before and after technology **deployment**.
- **Regular** review and monitoring of relevant processes, and performance ; regular review of new and emerging threats and evaluation of levels of risk
- Regular audit of relevant controls and **timely resolution** of audit findings

What Are the Characteristics of Effective Enterprise Security Governance?

What Are the Characteristics of Effective Enterprise security Governance?

- Do **decision making** and other key business processes take security concerns into account? *(eg. identified risks, and tolerable control of impacts and consequences)*

- Does enterprise security have an **appropriate level** of representation and agenda visibility on the executive management committee? For **board of directors**' meetings?

What Are the Characteristics of Effective Enterprise security Governance?

- **DO LEADERS** (directors, senior executives, business-unit managers) understand the key enterprise security risks facing the organization?

- Have clear and separate accountabilities for **enterprise-security governance** and management activities been **assigned?**

- Have enterprise-security strategies been **agreed** to and are they **understood** by IT, security (CSO, CISO, or equivalent), and business-unit managers?

What Are the Characteristics of Effective Enterprise security Governance?

- Conversely, does security management **understand** business strategies and priorities and reflect these in its **decisions?**

- Are **AWARENESS** and **EDUCATIONS** programs in place to ensure that the business gets the most value from enterprise security?

- Does enterprise security operate with the same risk-management processes as the rest of the business, and are formal processes **employed**—for example, is **Audit** involved when major changes are being made?

What Are the Characteristics of Effective Enterprise security Governance?

- Is there **evidence** that all employees understand the organization's security policies and procedures as well as the reason they are in place and **enforced?**

- Is security considered a **KEY** operating principle that is reflected in the **performance** expectations of the business?

Need an FOC assessment?

Thank You!