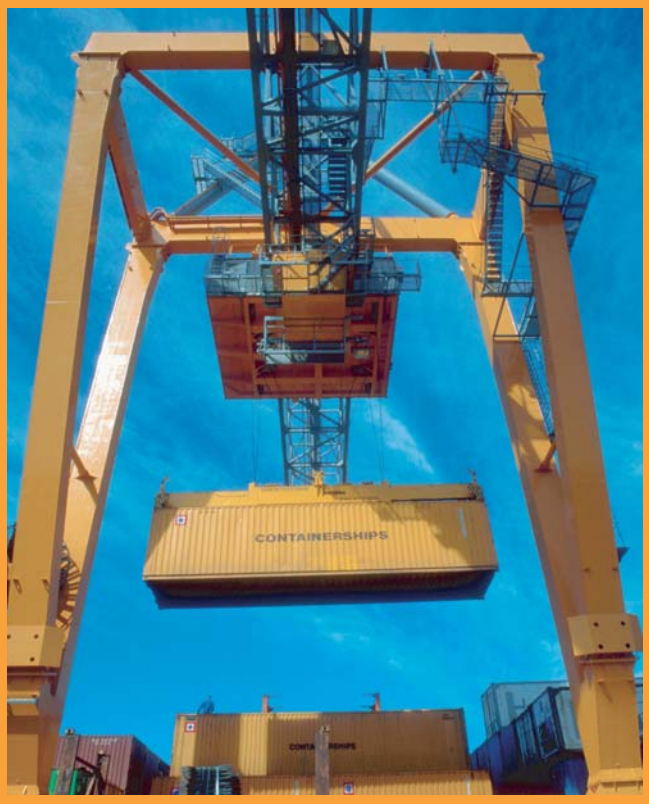
Threat & Vulnerability Management

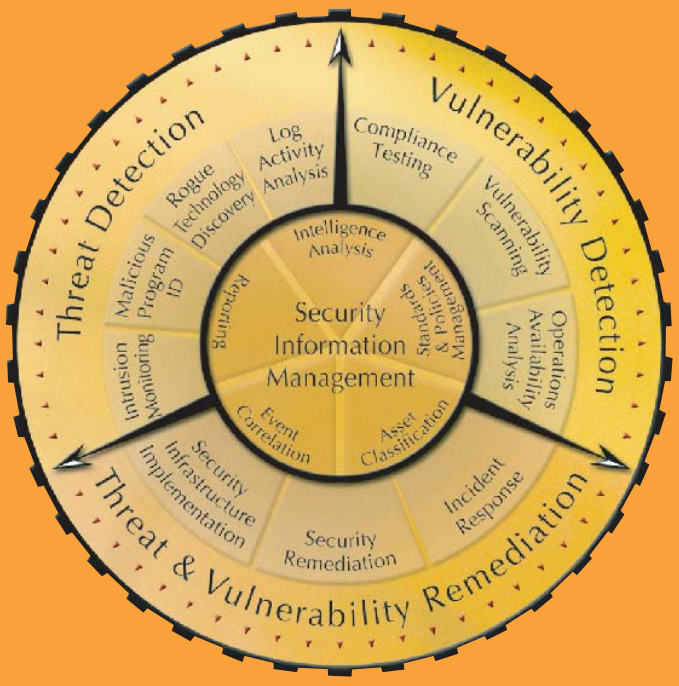


Nearly every enterprise now relies on information technology as an essential tool for meeting its business objectives. In so doing, however, enterprises must also contend with the various threats and vulnerabilities associated with today's computing environment. A threat can be defined as any event that might prevent or inhibit an organisation's ability to meet its objectives. Given these exposures, an effective strategy for threat and vulnerability management will include an integrated, proactive approach to protection.

Business Issues

Lack of attention to security threats and vulnerabilities can impact business in the following ways:

- Increased threats & vulnerabilities
- Greater potential for exploitation
- Insufficiency of basic firewall strategy
- Technology concerns
- Increased number of hackers
- Attacks are more sophisticated, and easier to launch
- Risk multiplier effect (both threats and vulnerabilities increasing)



*connectedthinking

PRICEWATERHOUSECOOPERS

Impacts

Following IT security issues have intensified the concerns of business executive management:

- Traditional security approaches obsolete
- Information assets increasingly exposed
- Valuable business transactions interrupted
- Stiffer penalties for security failures
- Inability to demonstrate a reliable control environment
- Threat life cycle decreasing (reaction time minimisation)
- Complex, heterogeneous computing environments increase risk and exposure
- New requirements for security controls
- Sarbanes-Oxley Act
- Various industry regulations

Threats in an IT security context are indications of impending danger to information assets, while vulnerabilities are susceptibilities to attack on IT systems. Proactive approaches anticipate the need for both threat and vulnerability detection, in addition to effective information security management. Threats and vulnerabilities are on the rise because of the growth of distributed computing environments, which make it easier to conduct remote, anonymous, and large-scale attacks. Web services, grid computing, shared storage systems, and peer-to-peer applications are all elements of this environment, and all add complexity to the problem of security management. Consequently, thorough security policy development, dissemination, compliance and enforcement become even more essential to ensuring system availability, data integrity and information confidentiality.

A PricewaterhouseCoopers comprehensive defence incorporates four primary activities:

- **Threat detection**
  Actively identifying and isolating threats to minimise their impact on assets.
- **Vulnerability detection**
  Actively identifying asset weaknesses before they can be exploited in an attack.
- **Threat and vulnerability remediation**
  Isolating and resolving asset security issues once identified.
- **Security information management**
  Integrating, interpreting, and presenting security-related information from disparate sources.

Benefits

Security management framework helps reduce risk of business interruption from IT security-related events through:

- Proactively identifying and responding to vulnerabilities
- Quick detection, containment and eradication of security incidents
- Leveraging the right people, processes and technology to reduce the total cost of ownership
- Using common IT security infrastructure components to reduce development time
- Demonstrating compliance with regulatory and best practice requirements
- Reduced cost of ownership by taking inefficiency out of the environment

To learn more about how we can reduce your company's security risks, please contact:

Pongsak Achakulwisut
Partner
PricewaterhouseCoopers
66 (0) 2344 1120
pongsak.achakulwisut@th.pwc.com
www.pwc.com/thailand