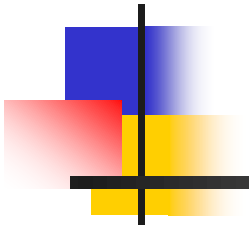
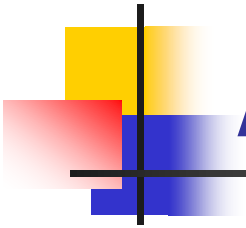


Security and International E-Commerce

Jim Maloney
jmaloney@SecurityPortal.com

November 2000

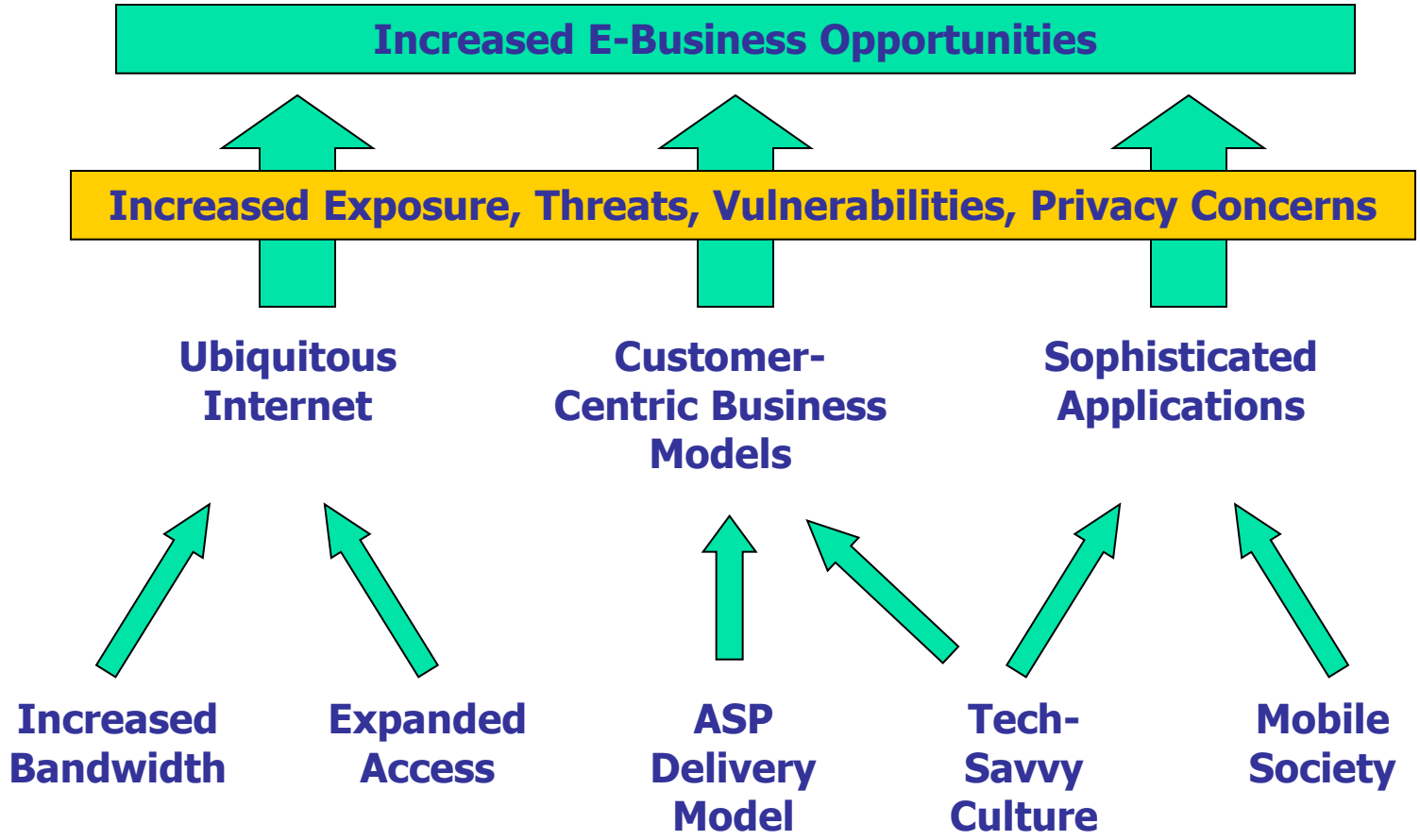
SecurityPortal
The focal point for security on the Net™

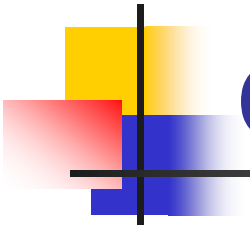


Agenda

- Security and e-commerce
- Security defined
- General security threats to e-commerce
- International security issues
- Key elements of a security solution
- Recommended security approach
- Summary

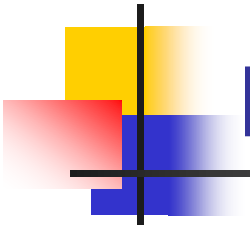
Why is security important for E-Commerce?





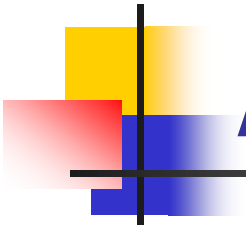
Old economy view of security

- In the "Old Economy" computing security was often viewed as a *discretionary* element of the business
- The focus was on *protection* of information systems and data



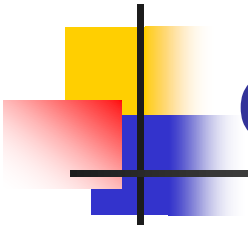
New economy view of security

- In the "New Economy" computing security is viewed as a *strategic* element of the business
- The focus is on enabling new ways of doing business and *value creation*
- And from a protection perspective, security is now protecting the entire business, not just its information systems



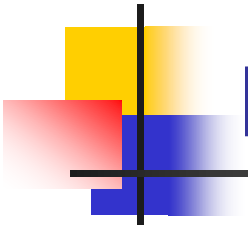
A working definition of security

- *Confidentiality* – the protection of private data on hosts or in transit
- *Integrity* - the system does not corrupt information or allow unauthorized malicious or accidental changes to information
- *Availability* - the computer system's hardware and software keeps working efficiently and the system is able to recover quickly and completely if a disaster occurs
- *Accountability* - the ability to determine who is responsible for the result of an action



General security threats to e-commerce

- Web site defacement
- Denial of service
- Theft of customer data
- Theft of intellectual property
- Sabotage of data or networks
- Financial fraud



Resulting business impact

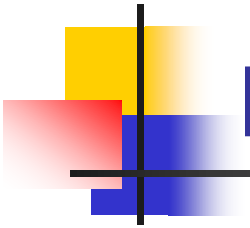
- Lack of consumer confidence if there are any real or perceived security issues
- Loss of profits due to last minute security implementations
- Damage to image and reputation if you have a visible security incident
- Bankruptcy if the majority of your business transactions occur online
- Benefits to competitors if your level of security is perceived to be inadequate

International security issues

- Regulations and policies
- Education and awareness
- Cultural norms
- Access modes
- Local government stance on cyber crime

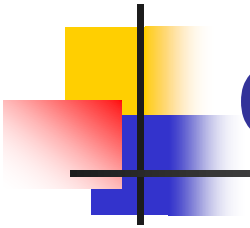
Regulations and policies

- Encryption laws vary greatly from country to country. This can impact both the availability and use of the appropriate technology.
  - http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm
- Privacy and consumer protection laws also vary greatly from country to country. These laws control how personal data can be used and shared. Can lead to substantial fines if violations occur.
  - http://www.gilc.org/privacy/survey



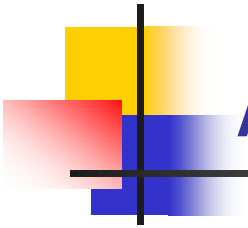
Education and awareness

- While malicious, external security attacks get most of the publicity, it is often employee mistakes and oversights that cause security issues
- Security awareness education for all employees, and specific training for your IT team, can be an excellent defense for both internal and external incidents
- A recent survey showed that 86% of Shanghai's networks had security products installed, but less that 2% of the network professionals actually knew how to protect their networks from intruders



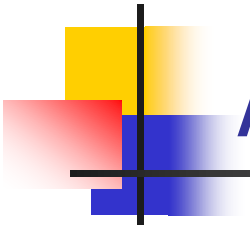
Cultural norms

- Limited work hours for support and emergency response services
  - Being "on-call"
  - Multi-shift operations (24/7)
- History of not protecting intellectual property
  - Electronic documents
  - Software
  - CDs and DVDs



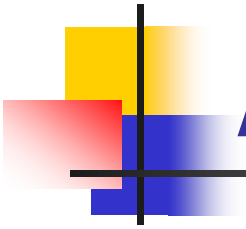
Access modes

- There is a rapid increase in the number of users accessing the internet via wireless devices such as cell phones
- In addition to their small size, portable wireless devices have limited processing power, limited memory and a limited power supply
- These characteristics lead to several security challenges



Access modes – continued

- With very limited keyboards and screens, cell phones and handhelds will require new authentication schemes to replace user names and passwords
  - New schemes may include screen-based biometrics, embedded certificates, hardware tokens, web cookies and PINs
- These devices are viewed as likely platforms for viruses that can be carried from network to network without detection

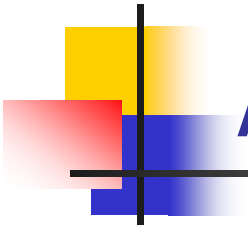


Access modes - continued

- Data moving through air is vulnerable to interception using relatively inexpensive equipment
- The portability of these devices increases the need for physical security and authentication

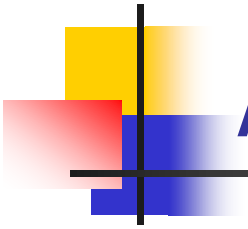
Local government stance on cyber crime

- Singapore – Very detailed statutes regarding penalties for criminal hacking
- Brazil – No special laws against cyber crime (and a very active hacking community)
- The Philippines had no anti-hacking laws until the "Lovebug" virus was traced back to their country
- Interpol is working to establish international standards for cyber crime legislation
  - http://www.mossbyrett.of.no/info/legal.html



Asia/Pacific perspective

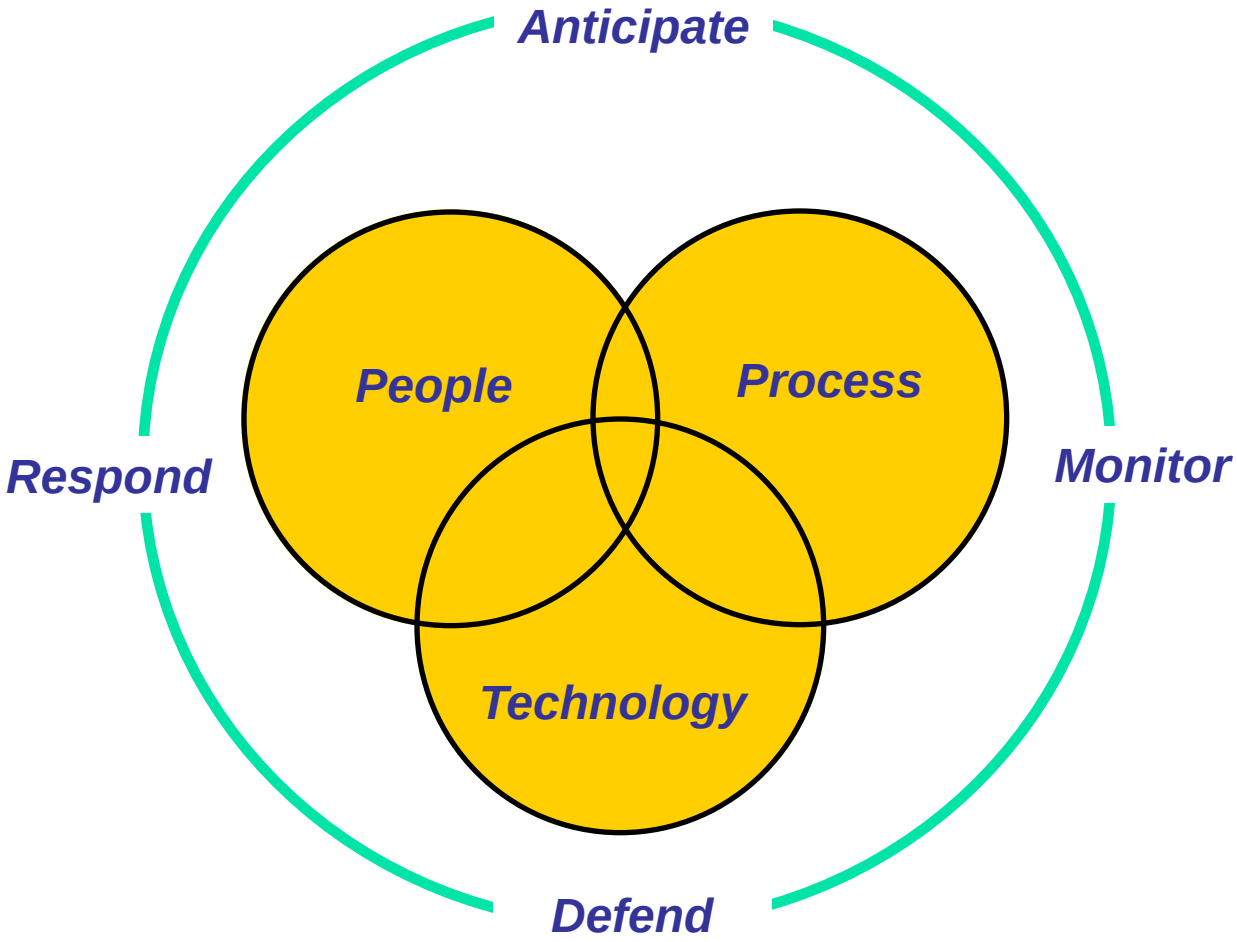
- Factors accelerating adoption of security
  - Growth of e-commerce in this region
  - Government initiatives supporting security
  - Recognition of the need for security guidelines, regulations and products that enable interoperability



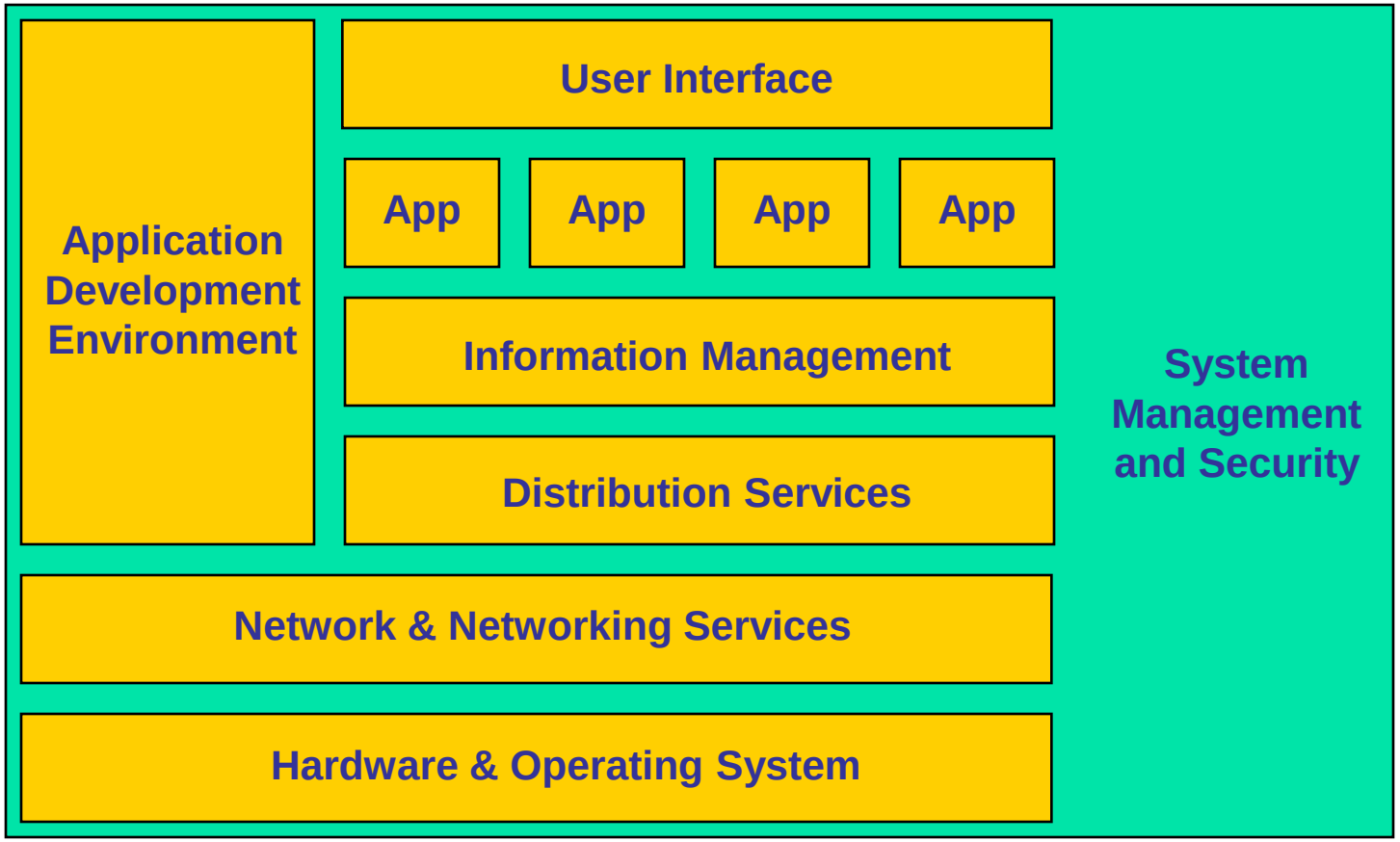
Asia/Pacific perspective - continued

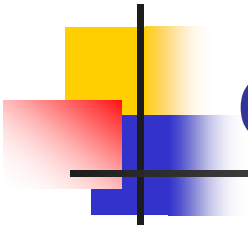
- Factors inhibiting the adoption of security
  - Lack of integrated security solutions that can span systems and regions
  - Lack of awareness of security issues and solutions

Security is more than technology



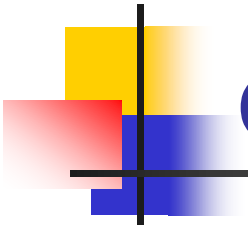
Security is an attribute, not a component





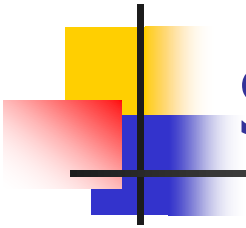
General security approach

- Develop accurate and complete policies that span the supply chain
- Make sure that all employees understand the importance of computing security
- Define clear roles and responsibilities for e-commerce security
- Perform regular audits, reviews and assessments of security
- Don’t ignore the physical security of your systems



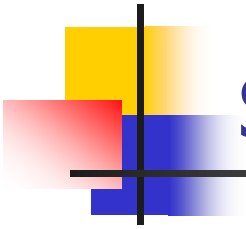
General security approach - continued

- Implement and maintain a set of baseline controls for your e-commerce system
- Implement user ID and authentication via strong passwords, secure tokens or biometrics
- Have backup and recovery plans in place



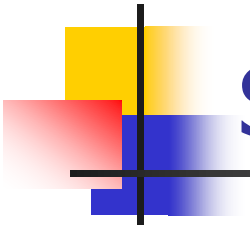
Secure web site development tips

- Include security as part of requirements gathering
- Include security as part of the architecture
- Be careful with embedded components
- Never trust incoming data
- Provide help to users
- Use code reviews
- Be aware of privacy and encryption laws
- Stay up-to-date on new risks, threat and vulnerabilities
- Document your security solution



Secure web site development references

- Recent articles on SecurityPortal: Best Practices for Secure Web Development (parts I and II)
- Web Security & Commerce (O'Reilly Nutshell) by Simson Garfinkel, Gene Spafford
- Web Security: A Step-by-Step Reference Guide by Lincoln D. Stein



Summary

- Security is a critical enabler for e-commerce
- The negative impact of poor security can be substantial
- Many of the issues and solutions regarding secure international e-commerce are people and process related, not technical
- Security is a key attribute of a system that must be designed in, not added on later
- Maintaining a secure web site requires continuous vigilance

Bibliography

- E-Business Security: An Essential Element in the Post-Year 2000 World. Gartner Group Research Report, April 17, 2000.
- The Net Present Value of Security. AtomicTangerine Special Report, October 11, 2000.
- International Ecommerce. SecurityPortal cover story, November 5, 2000.
- Information Security: The E-Commerce Driver. Dataquest Market Analysis, January 10, 2000.
- E-Business Impact on Security Technology and Practices. Gartner Group Research Note, November 11, 1999.
- Security Services in the Connected Age: From the basement to the boardroom. Gartner Group Market Analysis, July 4, 2000.

Bibliography - Continued

- Shanghai to Enhance Information Security. http://www.nikkeibp.asiabiztech.com, February 15, 2000.
- Wireless Security: Locking Down the Wavelengths. Information Security Magazine, October 2000.
- Do Handhelds Need Virus Protection? PCWorld.com, June 29, 2000.
- Best Practices for Secure Web Development. http://securityportal.com/cover/coverstory20001030.html, October 30, 2000.
- Best Practices for Secure Web Development: Technical Details. http://securityportal.com/articles/webdev20001103.html, November 10, 2000.