Integrating web application security control in the system development lifecycle

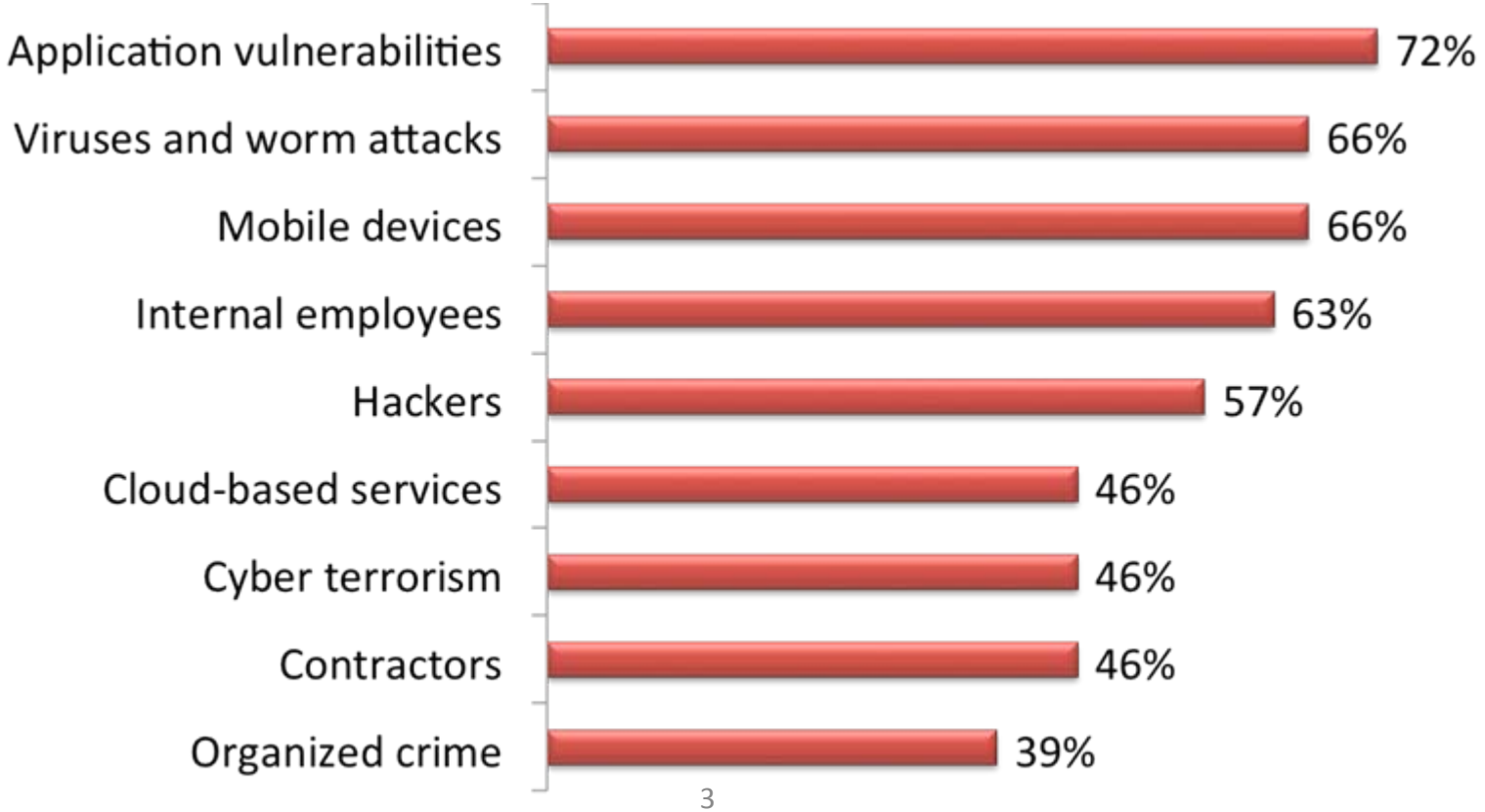
Chester Soong, CISSP-ISSAP, ISSMP, CISA
Managing Director
Security Consulting Services Ltd.

What are the Challenges

- Application security often receives much lower priority than it should in security planning
- Developers are under pressure from budget and time constrains
- Many of the application systems containing sensitive personal information, credit card data, and other sensitive corporate data are not thoroughly tested for data leakage and

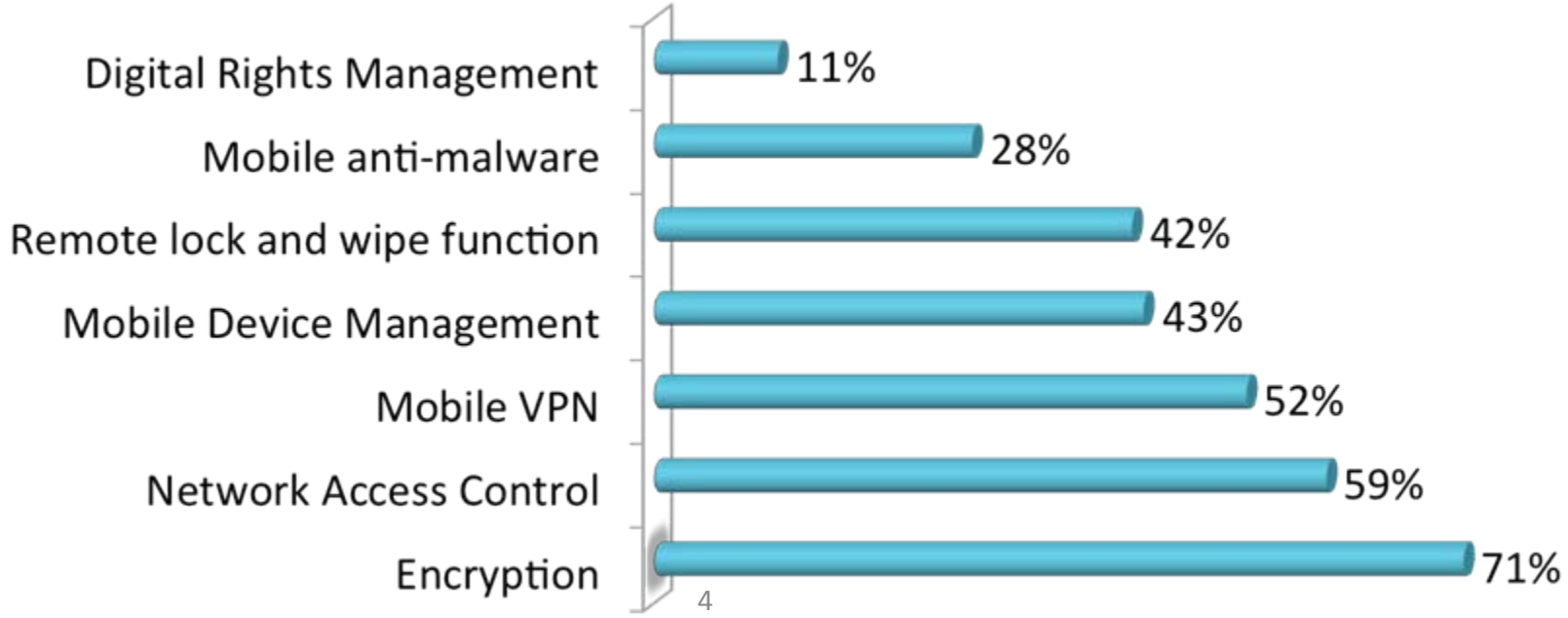
What We Learned – Top Threats

We need a paradigm shift in how security is considered across the enterprise to address the top security threats.



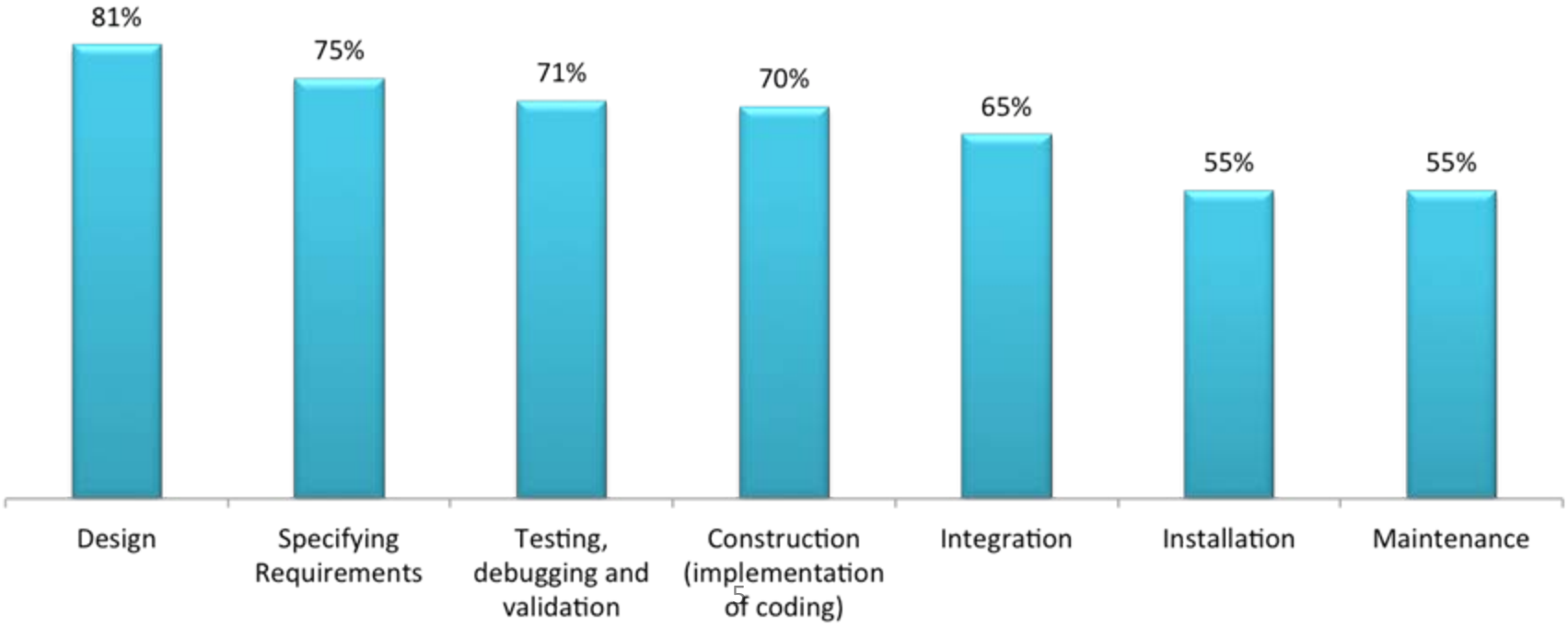
Changing Landscape - Mobile Devices

- 68% of respondents said Mobile computing devices are a significant risk to organizations.
- 69% have a formal policy in place to mitigate risks and use several solutions.



Changing Landscape - Application Vulnerabilities

73% of respondents identified application vulnerabilities as the top threat and have the following security concerns:



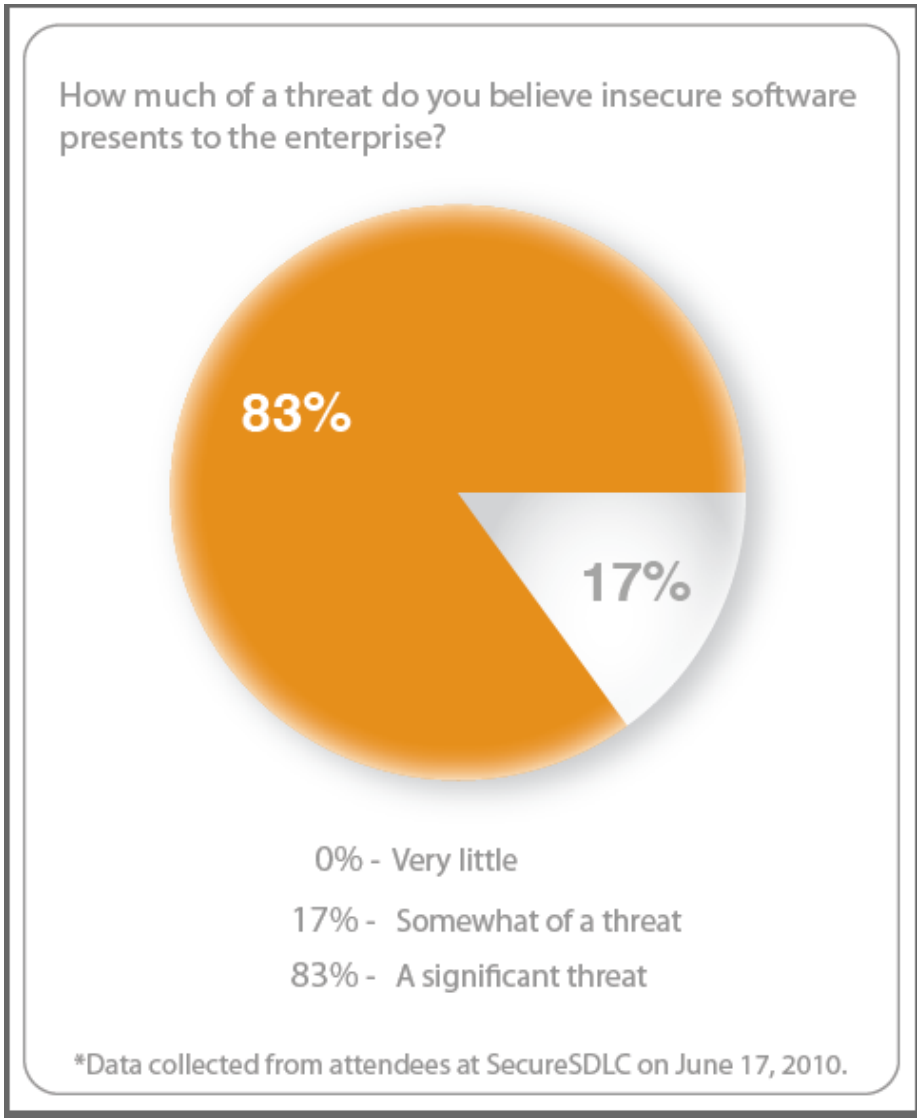
The Changing Landscape of Security

- Over 70% of security vulnerabilities exist at the application layer*
- Perimeter protection no longer sufficient – data compromise is the issue
- More incidents of data loss could result in greater government oversight and regulation
- 2008 (ISC)² Global Information Security Workforce Study report found significant costs result from data breaches
  - US $50 to $200 per record lost (not including reputation damage and loss of trust)

*Gartner Group, 2005

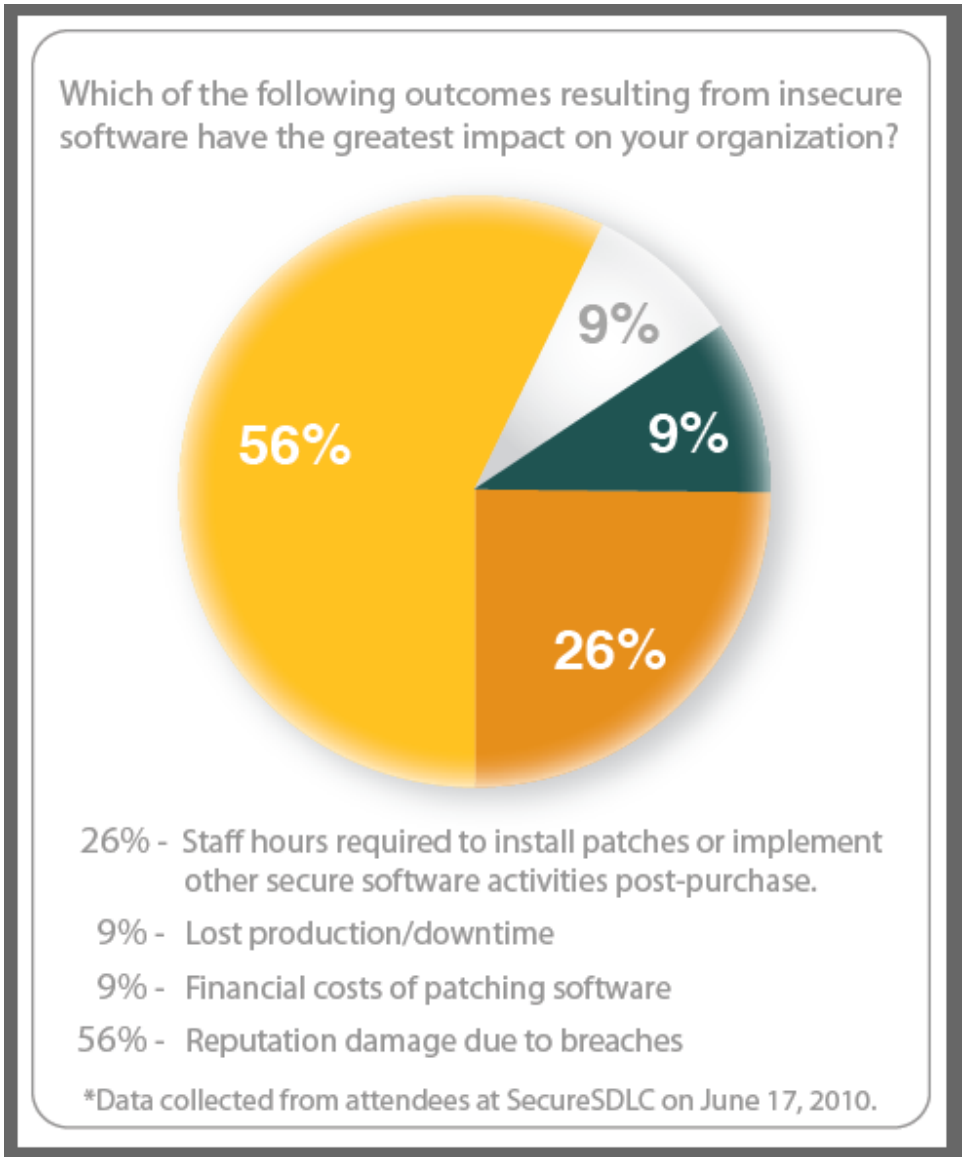
SECURITY CONSULTING SERVICES LTD

The Changing Landscape of Security

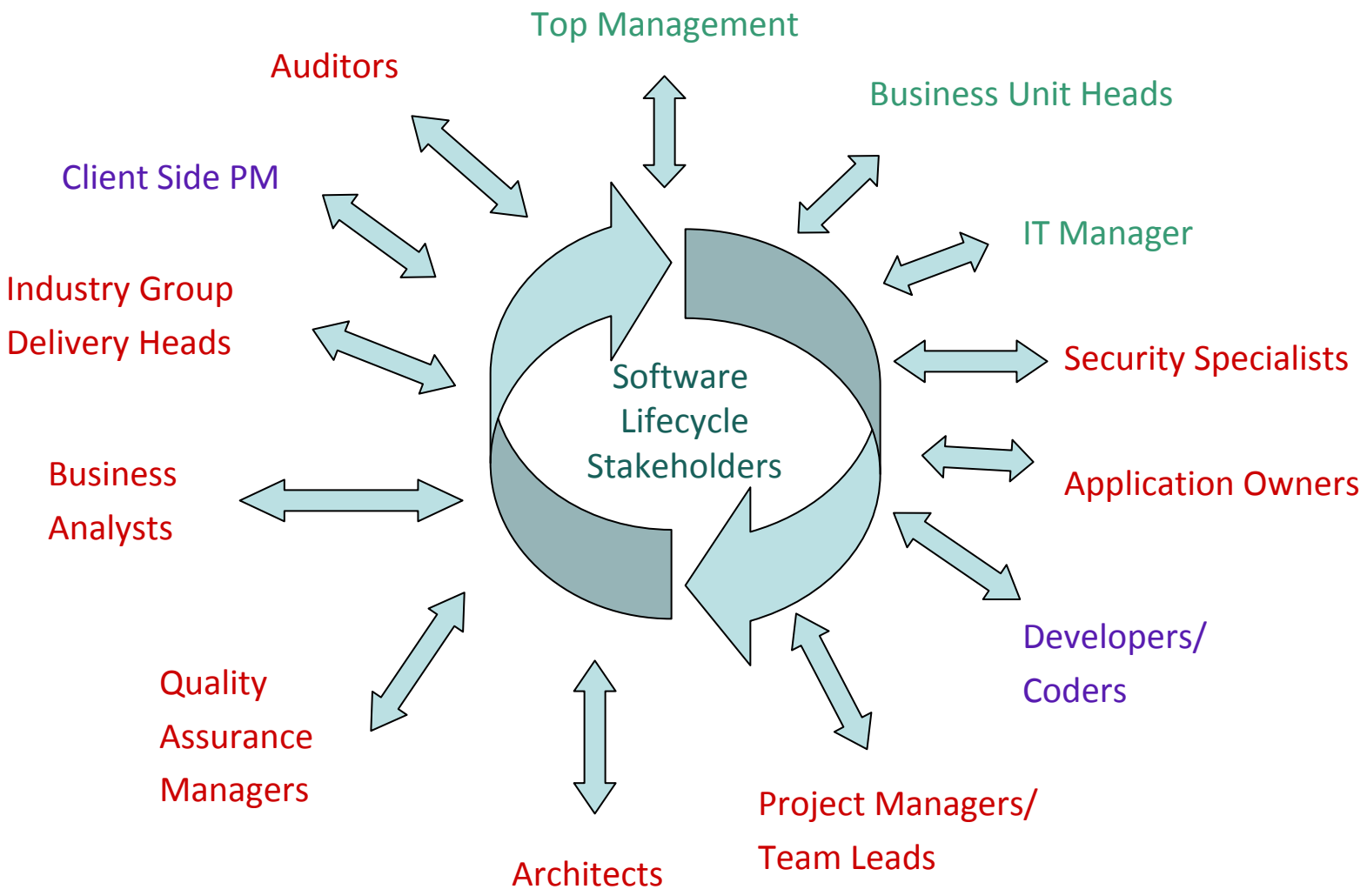


SECURITY CONSULTING SERVICES LTD

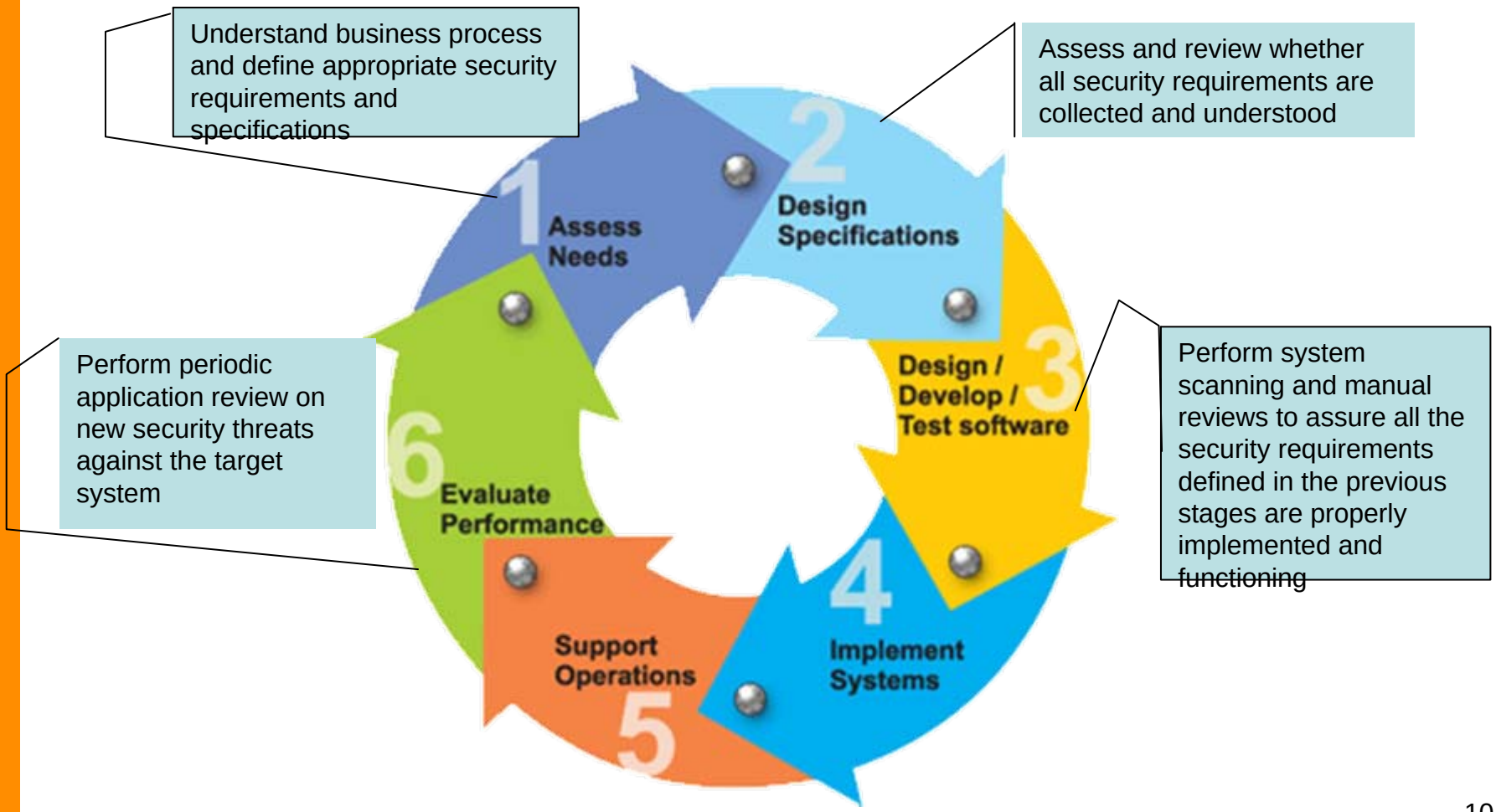
The Changing Landscape of Security



Software Lifecycle Stakeholder Chart



Perform Security Assessment and Audit during the SDLC



Objectives Achieved

- Avoid security requirement being missing in the design and as a result, not being built into the application
- Identifies application security issues before they are exploited
- Verify applications are properly configured and implemented to prevent sensitive or unnecessary information from being revealed
- Review application code for programming errors
- Validate user authentication processes, password reset mechanisms and session management schemes

Objectives Achieved (Cont.)

- Helps prevent application downtime and improve productivity
- Identifies specific risks and provides detailed recommendations to mitigate the issues
- Supports user confidence in application security
- Supports efforts to achieve and maintain compliance with government and industry regulations
- Regularly review the application to ensure no new vulnerability is affecting the system

SECURITY CONSULTING SERVICES LTD

Enhance your Development Staff's Capability in Application Security

- How do you make security a part of every phase of the SDLC?
  - Have educated people on staff.
- Variety of solutions but ONE that addresses from the holistic perceptive.
- Ways to address development:
  - IEEE: CSDA and CSDP (Software development)
  - SANS: GSSP-C, GSSP-J (Language specific/secure coding)
  - ISSECO: International Secure Software Engineering Council
    - CSSE (Entry level education program with certificate of completion given by International Software Quality Institute (iSQI)
  - DHS: Software Assurance Initiative (Awareness Program/Forum)
  - Vendor-Specific (ex: Microsoft, Symantec) based on internal lifecycle processes/technology specific

Purpose of CSSLP

- Addresses building security throughout the entire software lifecycle – from concept and planning through operations and maintenance, to the ultimate disposal.
- Provides a credential that speaks to the individual's ability to contribute to the delivery of secure software through the use of standards and best practices.
- The target professionals for this certification includes all stakeholders involved in the Software Lifecycle.

SECURITY CONSULTING SERVICES LTD

Thank you!

Email: chester@scshk.com