Security – Connecting the Trends!

Jan 30th 2010

Murali Krishna K
VP & Group Head – Computers & Communication Division
Infosys Technologies Ltd.

Emerging Innovation Trends……

- Connected Lifestyle
  - Social networking
  - Borderless sharing of Information
- Pervasive Computing
  - Increased footprint of intelligent devices
  - Network is the “Internet”, blurring boundaries
  - On-demand computing power.. Cloud based
- Digital Consumers & New Commerce
  - Mobility – Self Service – Personalization
  - Increased transaction volumes – New payment modes
- Smarter Organization
  - Simplify – Connect – Collaborate
  - Sustainability thru automation
  - Integrated security posture

Emerging Trends…… mapping threats

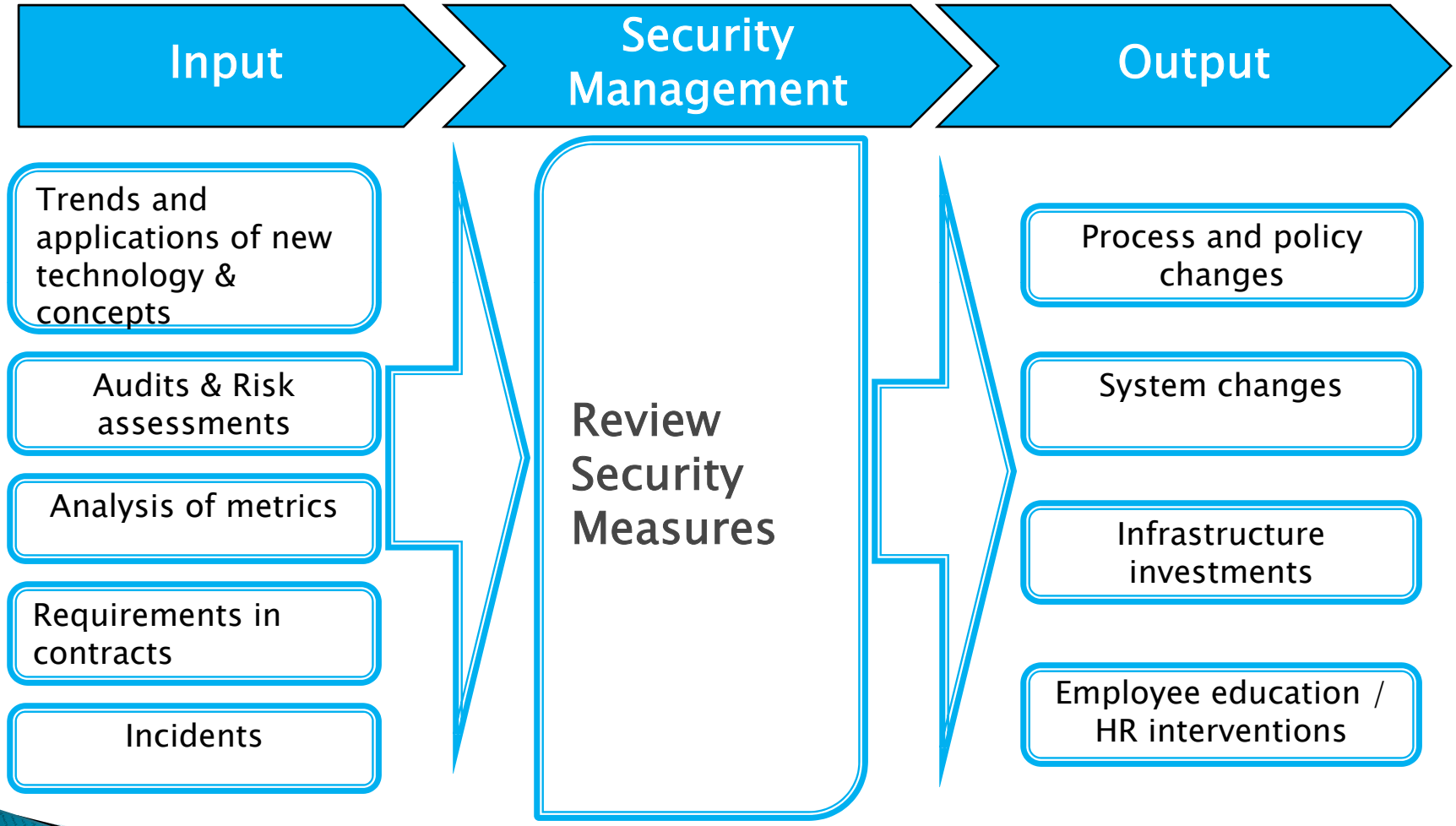
- **Connected Lifestyle**
  - Social Engineering – Identity & Intellectual Property thefts
- **Pervasive Computing**
  - Un-patched, wrongly configured devices
  - Access to compute power on demand with malicious intent
  - Poisoned community Images in virtualized environment
  - Data Privacy
- **Digital Consumers & New Commerce**
  - Identity Thefts and Targeted “for profit” attacks
  - Vulnerabilities at application layer
- **Smarter Organization**
  - Abuse of Access to information
  - Mobile/ Distributed workforce

Evolving Security Challenges …

- Insider abuse of access to data
- Theft of Proprietary Information
- Misuse of Internet access
- Infringement of Intellectual Property
- Virus, Worms, Spyware, P2P, ….
- Attacks on Internet exposed systems
- Unauthorized Software
- Physical access to facilities
- Securing virtual environments
- Securing end-points, network, content, application…..

… to be addressed thru right mix of Governance, Technology & Automation

Security Management Framework…



Mindset change…….
Reactive, Predictive & Proactive

Security by design, not an after thought… Illustrating a few activities,

- Formal **risk assessment** exercise of "what can go wrong" and "mitigation strategies"
- **Compliance** to the regulatory environment
- Readiness on a **continuous basis** and not on the eve of the audit
- Robust and independent **internal audit** mechanism
- Peer group collaboration for **pro-active** security posture
- **Regular** and periodic interaction with security agencies
- Continuous **Communication**
  - Awareness, quiz, channel for whistleblower, security tips, etc.

Security metrics…

Analysis-based continuous improvements with right measurements … Typical metrics applicable are,

- **Health Management** Metrics for systems (Desktops/laptops/server/switches/etc.) – Patches, Anti-Virus/Spam
- **Software management** Metrics – authorized/unauthorized, License compliance
- **Identity Life Cycle Management** Metrics – Access provisioning / revocation / monitoring
- **Reconciliation** Metrics – IT asset inventory with health management systems
- **Change Management** Metrics – Unapproved changes, Post facto approvals
- **Audit** Metrics – Compliance monitoring, configuration monitoring
- **Incidents** Metrics – Security incidents, data loss, IP and copyright violation
- **BCP & DR** Metrics – BCP Tests conducted, DRRs trained
- **Physical Security** Metrics – Access control, inventory control
- **HR** Metrics – Background verifications, disciplinary actions

In Summary…

We need the right mix of Governance, Technology & Automation

Patch Compliance from OS to

Application & Configuration compliance

Security Measures with monitoring to

Sense-and-Respond capabilities

Application development to

Trusted Application development methods

Security measures in Silos to

Integrated Security posture

Thanks

muralikk@infosys.com