RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Starting Over - Getting the Next Generation of Security Right

Dave Martin
EMC Corporation

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

Session ID:
Session Classification:

The legacy approach isn't working

- Built in & bolted on

- Single group responsible for security

How did we get here?

- Failure to address security requirements at foundational level, such as
  - Weak architectures reliant on
  - Most application logs are created for debug
  - Poor patching and application vulnerability
- Trust - or a lack of it (with good reason)
  - Poor education of true threat and risks
  - Believe we are the only ones that can perform security functions
  - That risk can mostly only be addressed in our own additional layers of technology

Some examples

- There are good reasons to use these technologies but often they are used instead of addressing the root cause…
  - Web application firewall
  - Network / endpoint data loss prevention
  - Vulnerability scanners
  - And more…

What is the downside?

- Root causes remain unaddressed
- The security infrastructure is complex and static
  - High cost of operations
  - Agility is impacted or requires massive automation
  - Control complexity leads to error and failure
  - Tendency to adopt non standard designs
- Infrastructures cannot keep pace with technology and business evolution
  - Mobility
  - Cloud

A better way forward

- Build it in, not bolt it on
- Truly make security EVERYONE's responsibility
- Trust, but verify

Build it in, not bolt it on

- Reusable API's to embed controls in the application
- Hypervisor based controls in virtual environments
- Create intelligent threat and risk focused log facilities

Security is EVERYONE's responsibility

- Educate IT and business functions on threat, risk and standardized controls
- Produce standard risk / control mappings
- Introduce new mechanisms to drive preferred control implementation
  - Solution defense and detection requirements
  - Measure and goal against successful implementation
- Measure and show benefits
  - Agility
  - Cost effectiveness
  - Control effectiveness

Trust, but verify

- Establish controls assurance capabilities
  - Measure
    - Design Quality
    - Control reuse and standardization
    - Presence
    - Effectiveness
  - Dashboard reporting
  - Alert and respond for control failure or drift

Change doesn't happen overnight

- This is a major cultural change for most security and IT organizations
- Like all change, key elements
  - Executive sponsorship
  - Measure and goal for success
  - Drive accountability
  - Don't expect to change everything/everyone at once
- Leverage other projects with similar goals
  - Cloud
  - Mobility

Thank You

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012