Security Risk Management Strategy in a Mobile and Consumerised World

RYAN RUBIN (Msc, CISSP, CISM, QSA, CHFI)
PROTIVITI

Session ID: GRC-308
Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

AGENDA

- Current State
- Key Risks and Challenges
- Opportunities
- Practical Next Steps

CURRENT STATE

THE WORLD HAS CHANGED

- Consumerisation of IT
- Younger workforce
- Mobile workforce
- Web services
- Outsourcing / Offshoring
- Cloud computing
- Regulatory environment
- Economic pressure
- Political risk

Lined up outside the IT department for a Blackberry?

Verizon breach report 2011 * 2012 **

ISACA Cloud Survey 2011 **

InfoSec Europe '12: Dr. Paul Judge ***

INTERESTING STATS

Security Breaches

- 96% of attacks in 2011 were simple*
- 97% could have been prevented by rudimentary controls*

Cloud Computing

- 45 % risks outweigh benefits**
- 38% benefits and risks are balanced
- 17% benefits outweigh risks

Mobile Computing

- Est 50 billion apps downloaded this year
- Mobile malware increased 700% in a year
- 1 million new iPhones and Android devices purchased daily

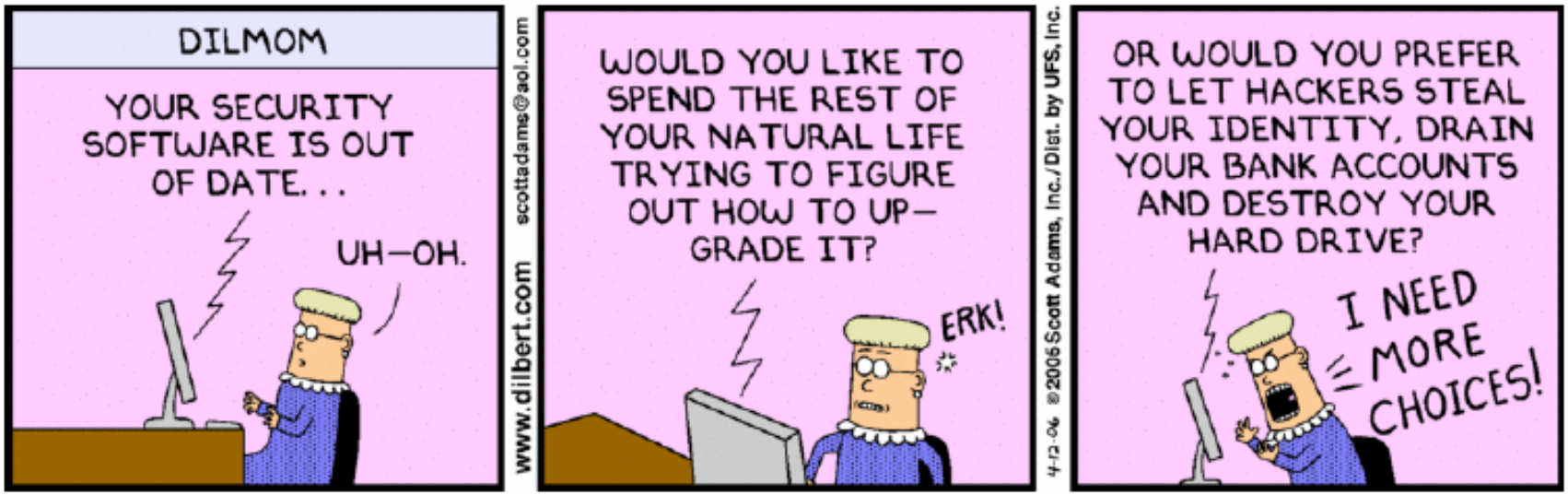
Social Media

- 1 in 100 posts on Twitter are spam / malicious ***
- 1 in 60 posts on Facebook are spam / malicious ***
- 20 % of all Facebook users are active targets of malware.
- 47% have been victims of malware infections

Outsider Threat

- 98% breaches stemmed from external agents*
- Only 4% implicated internal employees *
- 58% data theft tied to external agents
- ¼ London Wifi spots still insecure

WHY IS INFO SEC NOT WORKING?



WHY IS INFO SEC NOT WORKING?

- Governance and management support
- Over compliance and regulation
- People weakest link
- Supportability of new technologies
- Organisational culture
- IS efficiency and effectiveness
- Poor visibility and awareness

RISKS AND CHALLENGES

RISKS IN OUR NEW WORLD

- Loss of control over HW and SW
- Attacks target users through social networking, mobile apps, browsers, drive by downloads, search engine poisoning
- Opening our Infrastructures for external access
- Data leakage and data loss opportunities
- 3rd parties and cloud providers
- Shadow IT

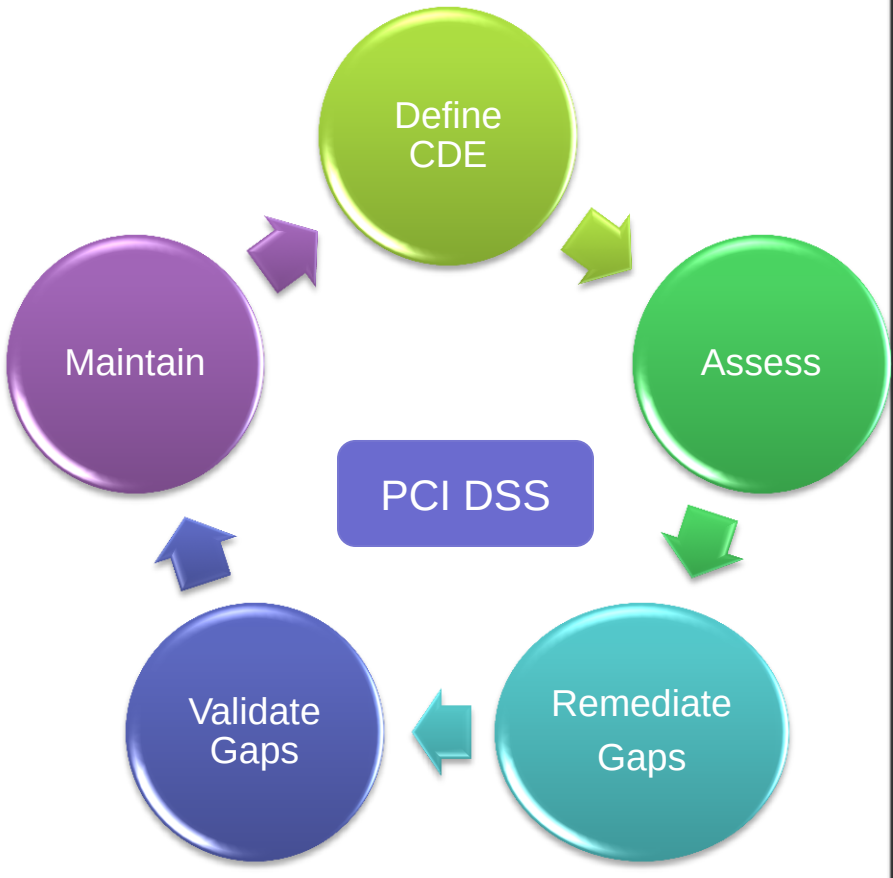
RESETTING EXPECTATIONS

- 100% security is possible

EXISTING FRAMEWORKS

Scope: All Information Assets within ISMS

Control Framework: ISO27002



Scope : Cardholder Data

Control Framework: PCI DSS

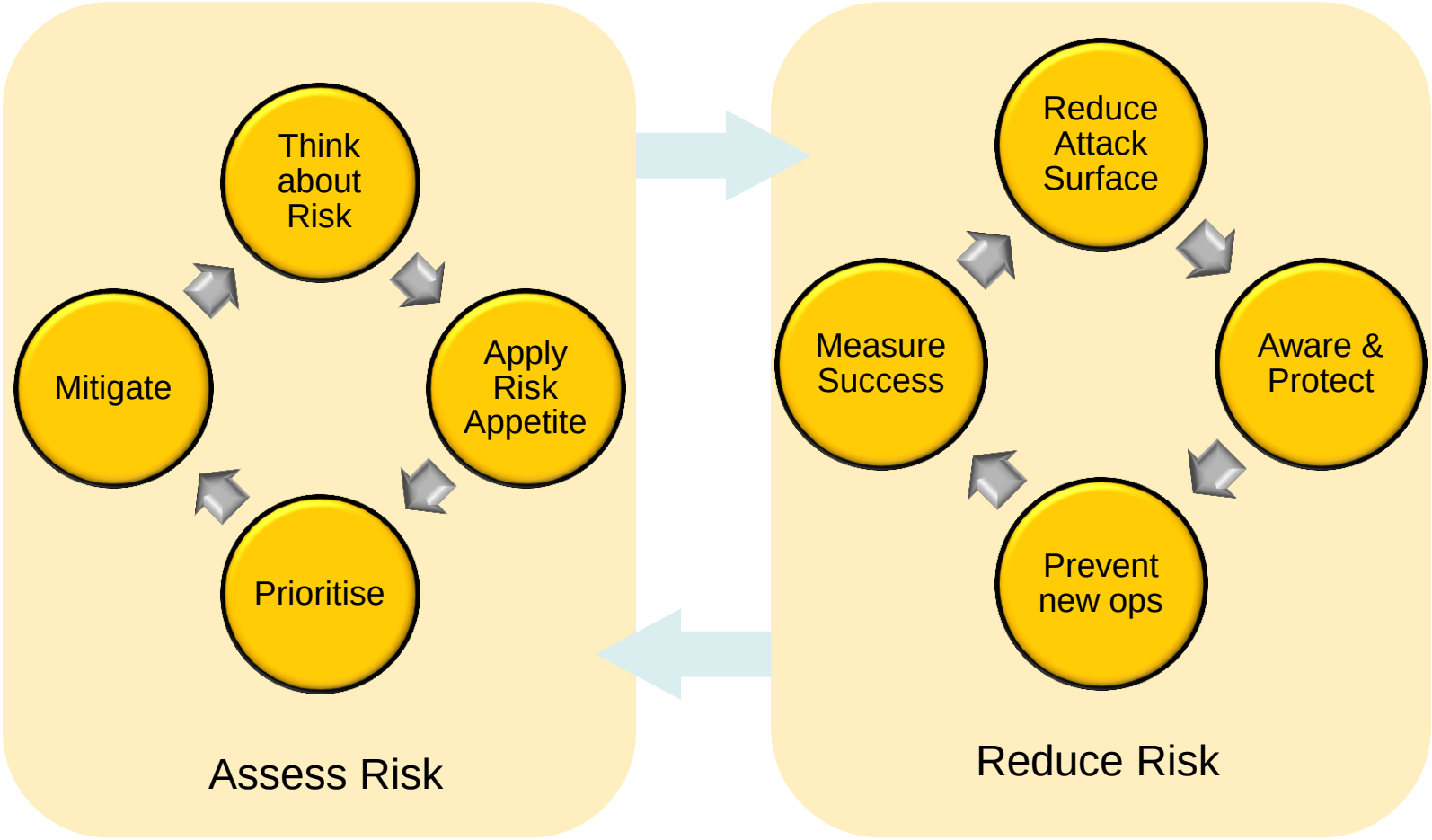
OPPORTUNITIES

DUTY OF CARE

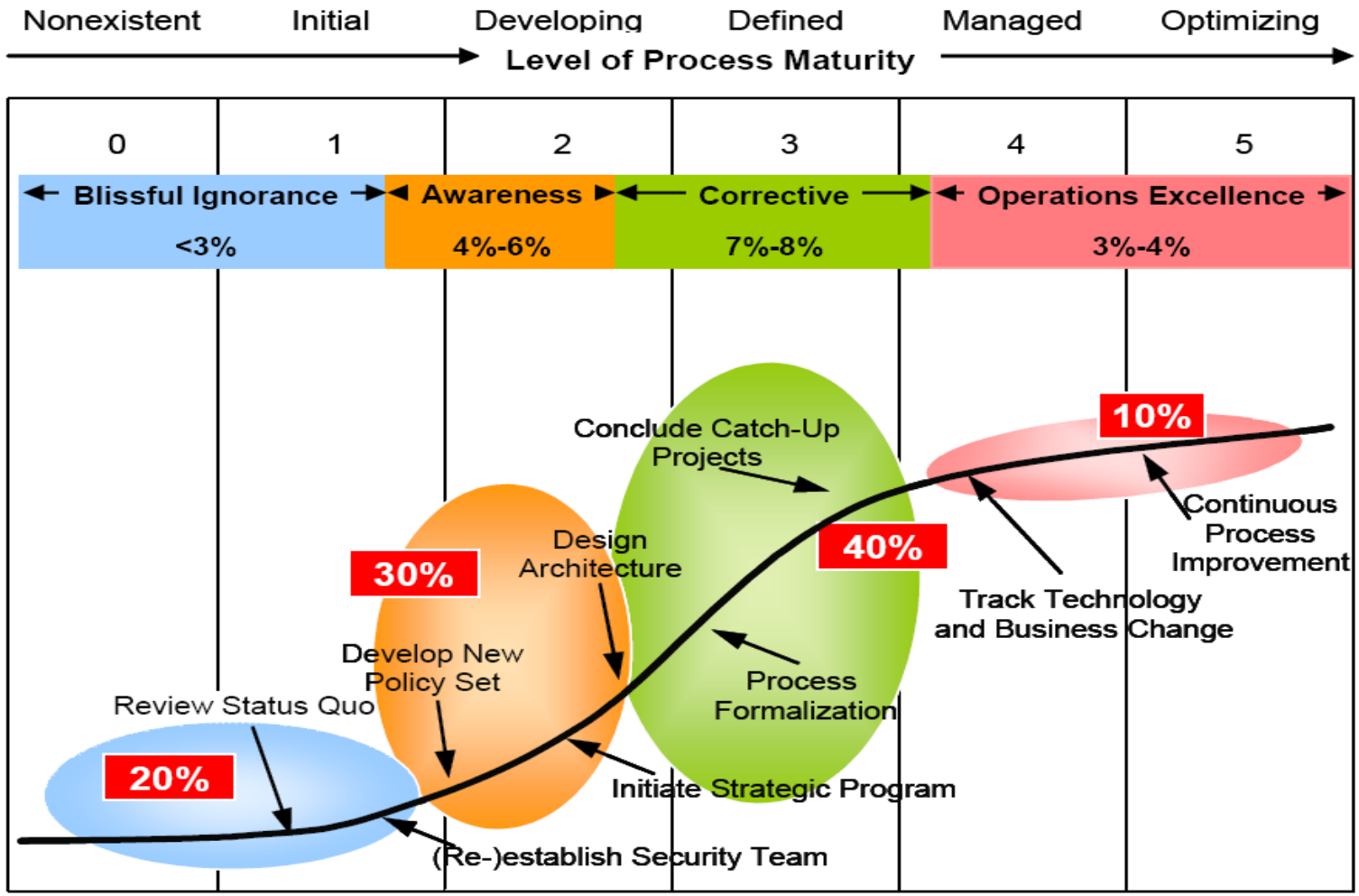
- Protect customer data
- Maintain controls for crime prevention
- Reduce risk to operations and information assets
- Know and understand legislation and regulations
- Accountable and liable for non compliance
- Retain and protect all records needed
- Ensure confidential information is not disclosed

UK DPA - COMPANIES ACT – COMPUTER MISUSE - FRAUD

AGILE APPROACH TO SECURITY



WHERE ARE YOU ON YOUR JOURNEY ?

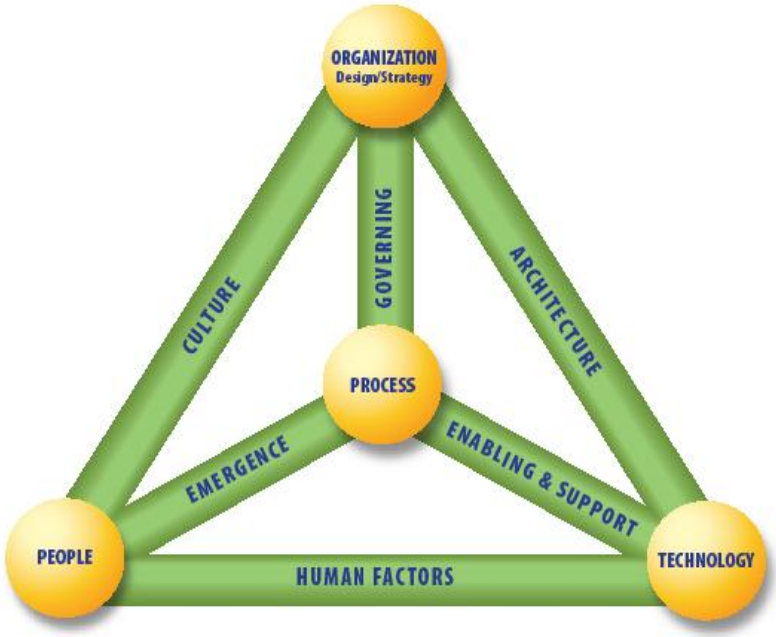


Note: Population distributions represent typical, large G2000-type organizations.

Source: Gartner (March 2007)

AGILE BEHAVIOURS

Step function thinking	Culture and behavioural change	Prepare for failure
Defensible position	Apply cross functional skills	Security Inside™
Focus on selling security	Better intelligence applying risk based decisions	Wider engagement
Rapid organisational response	Report right things	Better collaboration



CASE STUDIES

European Airline

* Focus on reputation

Global Publisher

* 3rd party assurance

Global Mining Company

* Minimum standards & checklists

Global Media Company

* Measure against Top 10 Controls

Global Recruitment Firm

* BYOD mobile devices
* Social Media Policies

Global Shoe Retailer

* 8 week group huddles

BABY STEPS: SECURITY 80/20

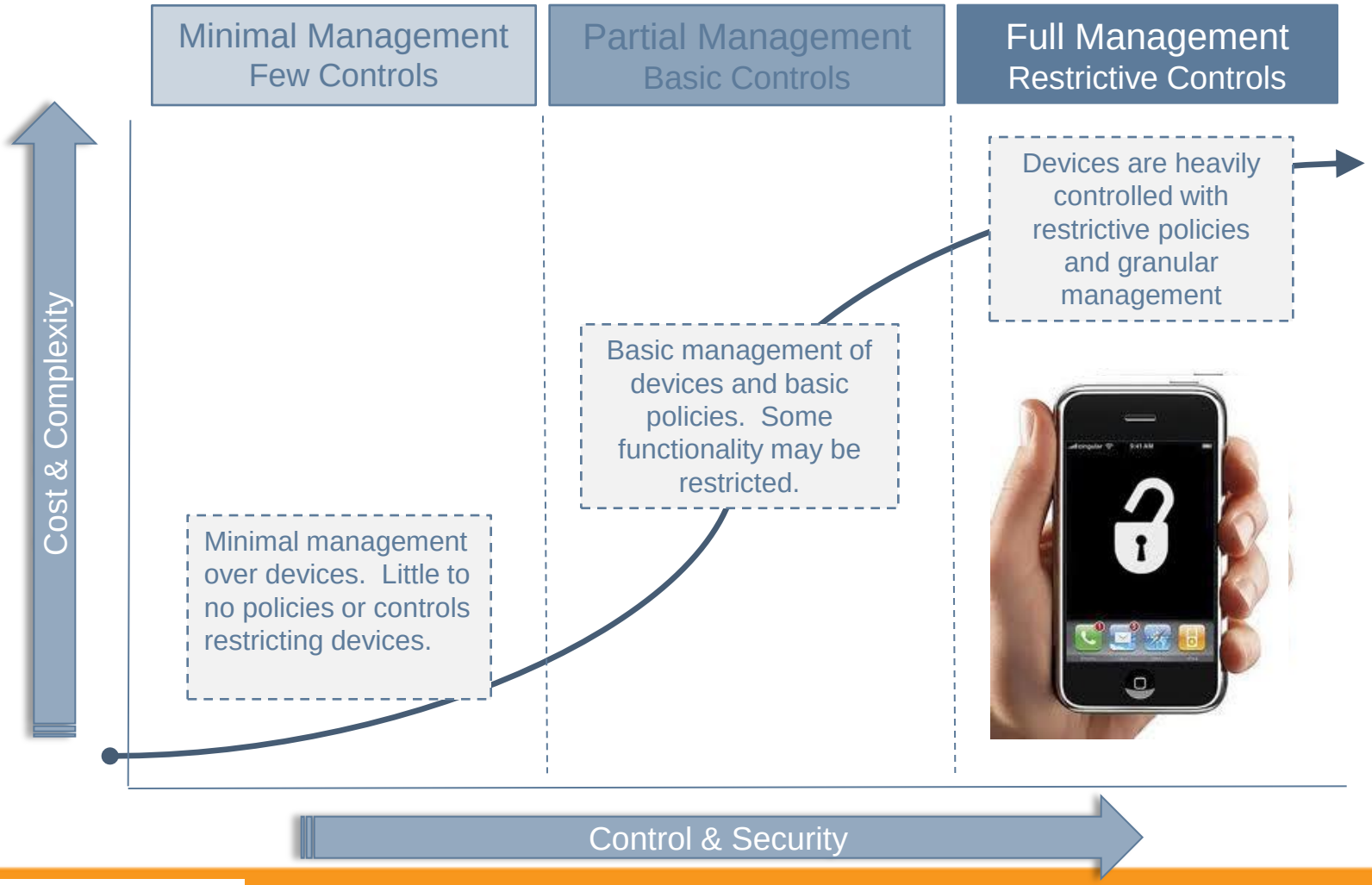
1. UNDERSTAND RISK APPETITE & CULTURE
2. CREATE IMPROVEMENT PLAN
3. DEFINE AND UPDATE POLICY
4. APPLY GOOD (P) RACTICES

PCI DSS	**PEOPLE**	**PERIMETER**	**PENETRATION**	**PROACTIVE**	**PEOPLE**
PROXY	**PROGRAMMING**	**PROTECTION**	**PROCUREMENT**	**PASSWORDS**	**PATCHING**

PRACTICAL STEPS: MOBILE DEVICES

- Create Formal Policies for Mobile Devices
- Create Your Own App Store
- Control Wireless Access
- Consider Network Access Control
- Consider Creating a Policy Server

BALANCING FLEXIBILTY vs CONTROL



PRACTICAL STEPS - CLOUD

- Privileged User Access Management
- Regulatory Compliance
- Data Location
- Data Segregation
- Resilience, Recovery, Continuity
- Investigative Support
- Long Term Viability
- Accreditation

REDUCING SECURITY RISKS

Security Risks	Risk reduction strategies
Web application security	Software development lifecycle, education, due diligence, testing
Social media networking	Policy, Awareness, Technology
Advanced persistent threats	Raise the bar as best as you can
Mobile applications	Awareness, Technology, Process
Insider threats	Risk assess key assets and people, appropriate controls
Information security function effectiveness	Stop putting out the fires – educate people not to smoke.
Cloud Computing / 3rd party providers	Due diligence – choose your partners wisely
Over compliance and regulation	Be pragmatic and sensible – think longer term
Lack of security awareness	Create awareness and embed
Younger workforce	Awareness, appropriate controls

SORRY - NO SILVER BULLETS FOR SALE

MEASURING PROGRESS

- So what?
- Aligning exposure with tolerance of business

Risk	Key Risk Indicator	Key Performance Indicator
Confidentiality (Manufacturing)	% deals lost to competitive intelligence	Competitiveness Index
Privacy (Insurance)	% of incidents where customer data at risk	Customer satisfaction and renewal indices
Availability (Manufacturing)	% of lost inventory due to system downtime	Manufacturing Capacity Index
BCM (Healthcare)	% DR plans tested	Bed mortality rates

APPLY SLIDE

- STOP using vulnerabilities and gap lists
- GET BUY IN from top
- ENGAGE with people to MANAGE expectations
- UNDERSTAND risk landscape
- ESTABLISH risk threshold
- BALANCE security with appetite
- SIMPLE security first
- CHOOSE your partners wisely
- EDUCATE responsible behaviour
- COMMUNICATE effectively
- MEASURE performance, refine and improve

"It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

– Warren Buffett

Powerful Insights.
Proven Delivery.™