Microsoft CISO Perspective: How We Protect Microsoft

Miguel Caldas
CTO
Microsoft Portugal

Our Goals

Dialogue

Share

Learn

Trends Shaping Our Company

Evolving for the future

Workforce
~90K Employees
~180K End Users
~94K Win8 + IE10 systems
~102K Office 2013 clients
~880K SharePoint Sites
85% use Lync for voice

Multi-Generational
40 %- Boomers

40 % - Gen X'ers

20 % - Millennials

Connected
94K Mobile Email
66% on Twitter
90K Windows Phone
6K Macs
9K iPhone
5K Android
5K iPad
75K MSFT Yammer

Global
112 Countries
~40K non-US Employees

The Road Ahead:

Services, Devices and Connectivity are vital to our success

1. Industry Trends

- The unprecedented scale of cloud computing is eroding the effectiveness of traditional security controls
- The broad adoption of consumer devices and services greatly limit our ability to implement new controls

2. Greater Intelligence

- Our assessment and monitoring investments have helped us gauge the effectiveness of our defense in depth model
- We have keener insight into the technical interdependencies of our critical systems and assets

3. Evolving Adversaries

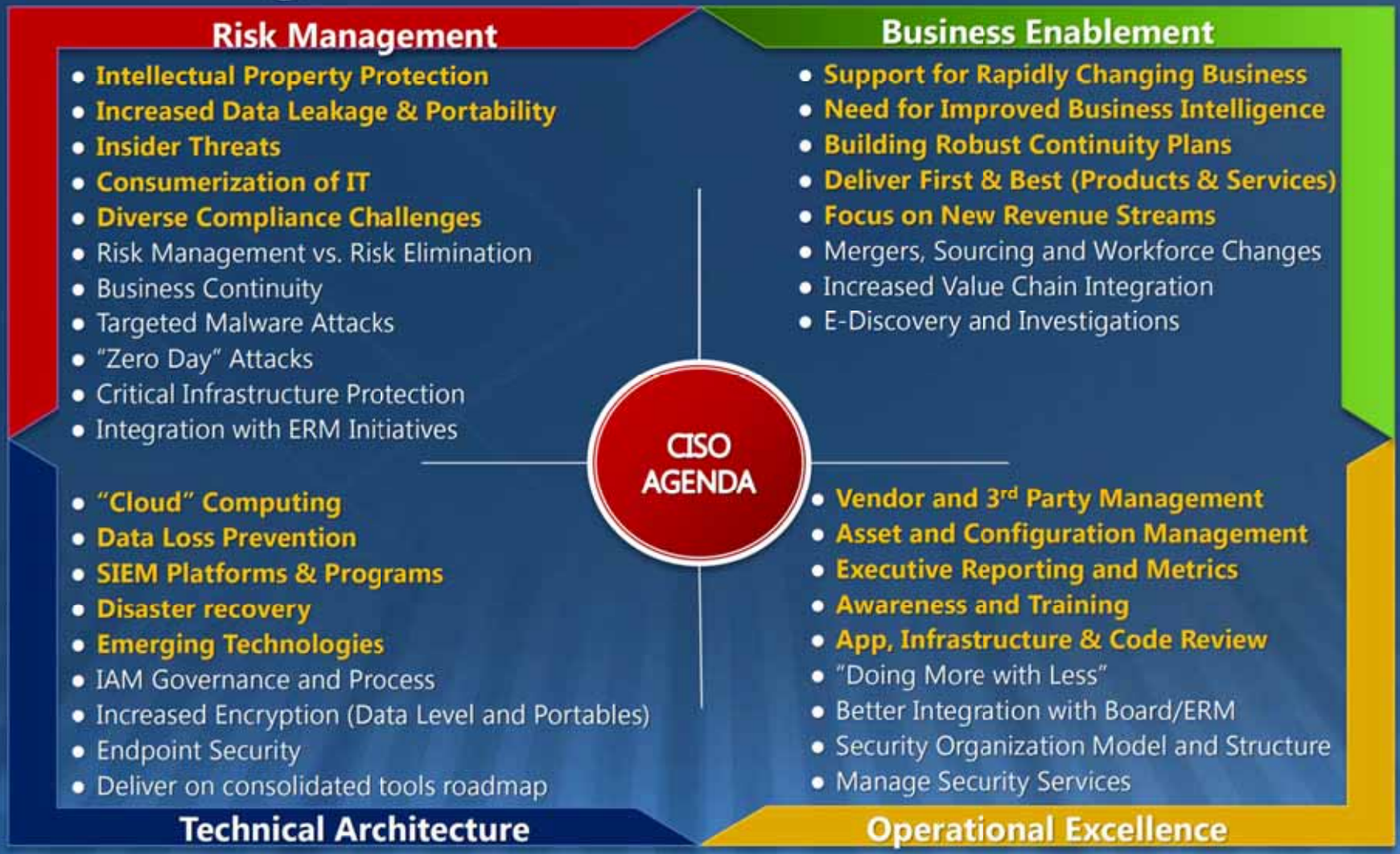
- Compromises focused on IP theft, financial gain, and hacktivism are on the risk
- Specialized and custom attacks are pervasive and available

4. Acute Need to Adapt

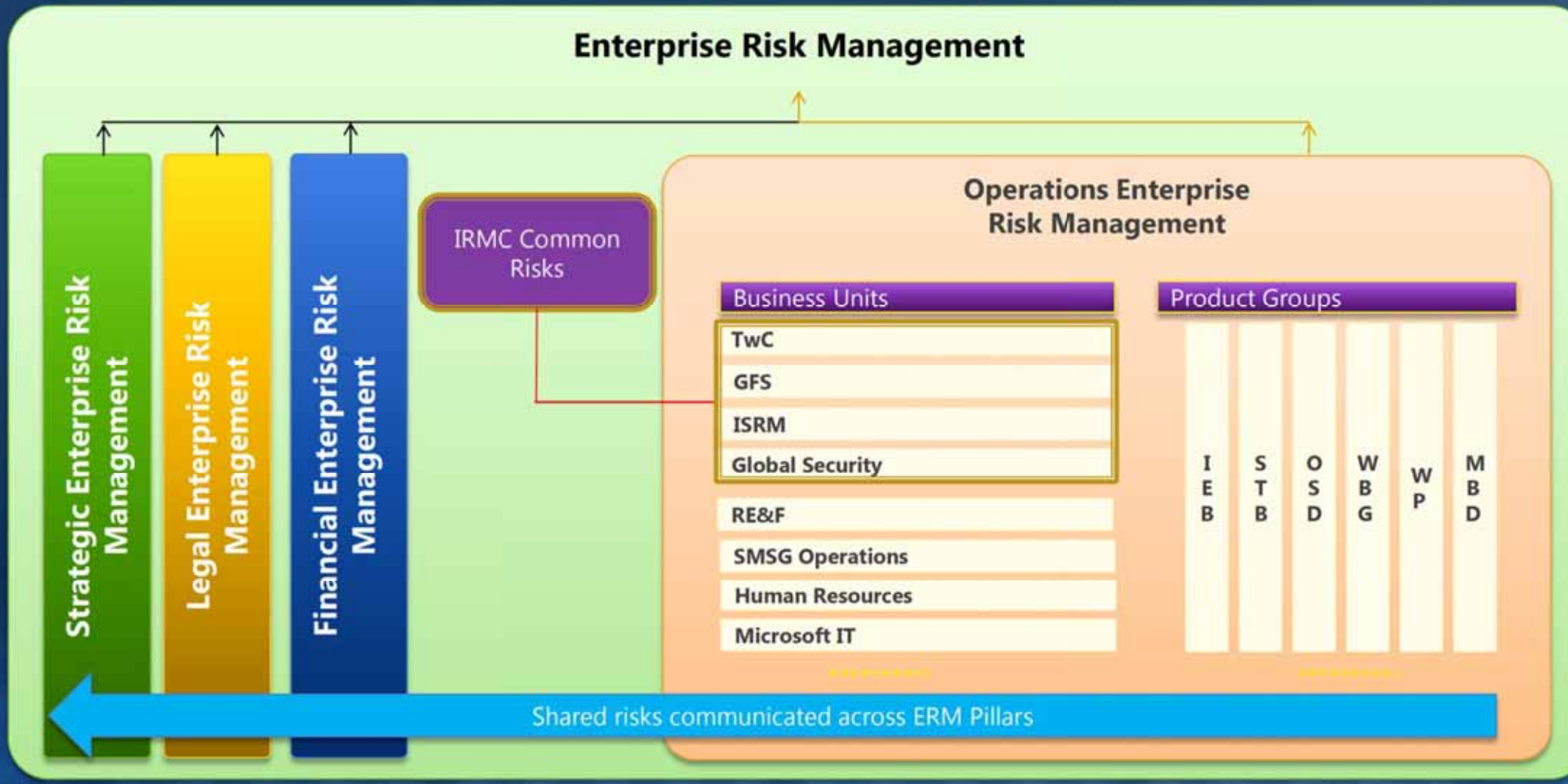
- We must act now to enhance the protection of our most critical assets
- We have a clear need for more consistency and rigor in isolating these assets

Our risk landscape is rapidly changing– Existing controls and processes must evolve

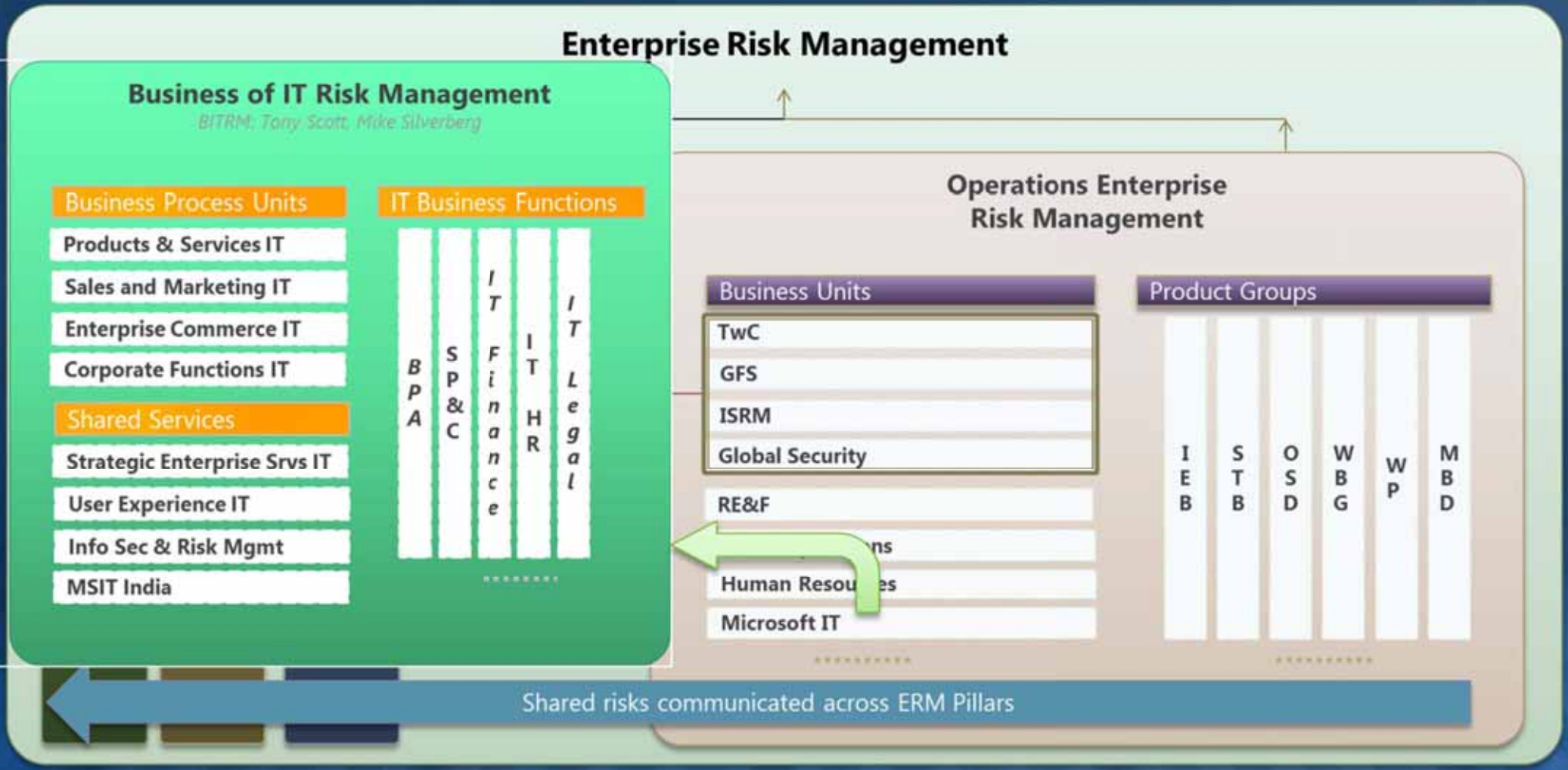
The CISO Agenda



OERM Annual Risk Assessment

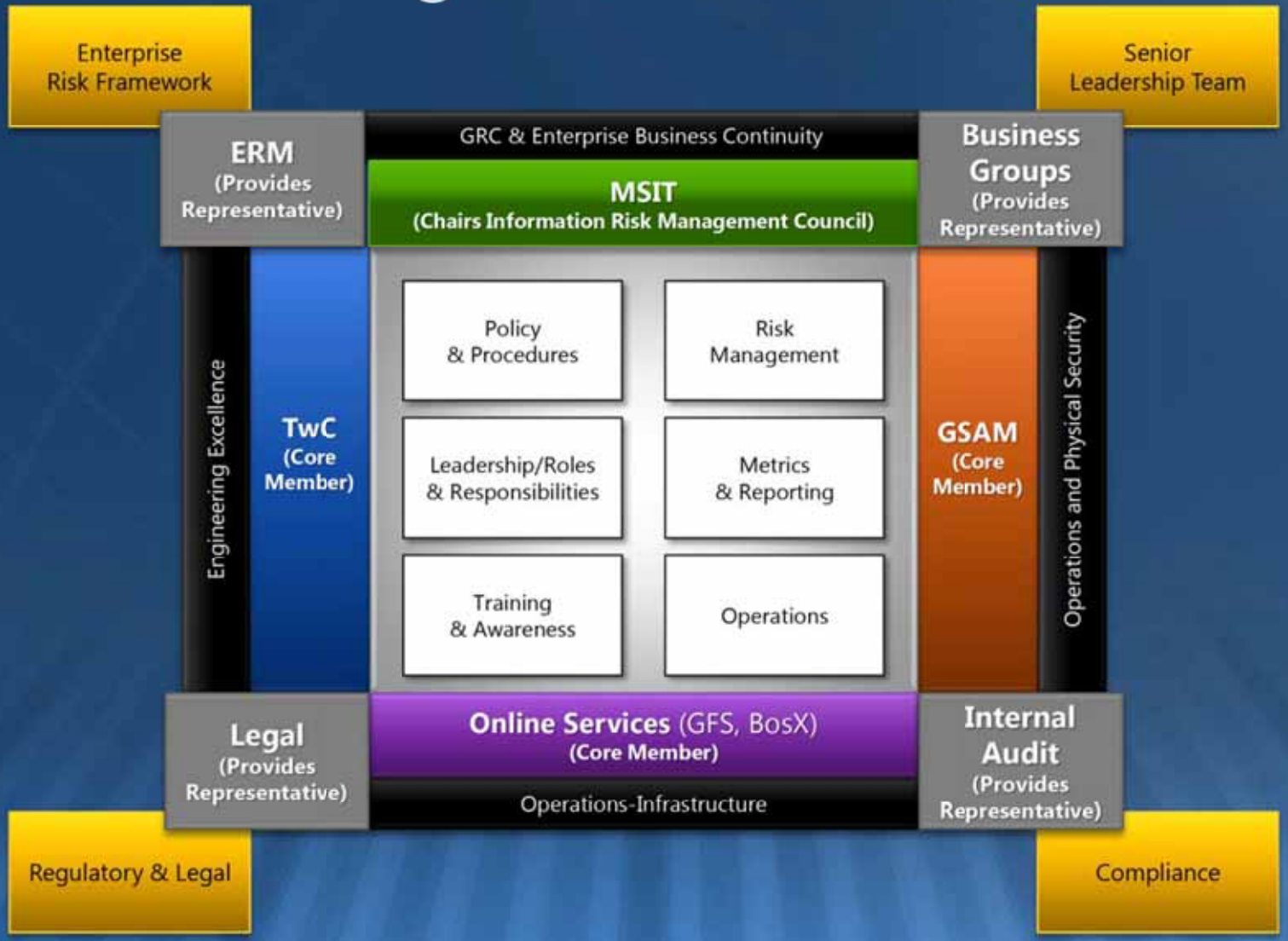


OERM Annual Risk Assessment



Microsoft Security Organizations

Information Risk Management Council



Information Security & Risk Management

All information and services are protected, secure and available for appropriate use through innovation and a robust risk framework

IMPERATIVES

PROTECT	ACCELERATE	DRIVE	OPTIMIZE	ALIGN	SERVE
corporate assets	risk management	security standards	the organization	practices/business	our customers

Governance, Risk & Compliance

Security Accelerators for Emerging Technology & Threats

Security Operations

Business Continuity

Assessment, Consulting & Eng.

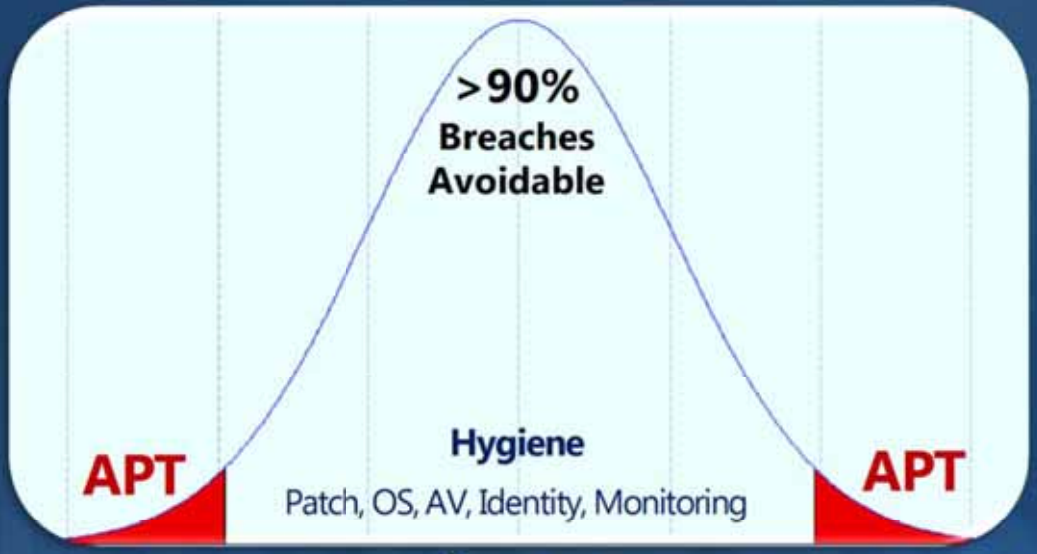
Tools

Cyber Security & Resilience

Current Trends: Not "If"... "When"

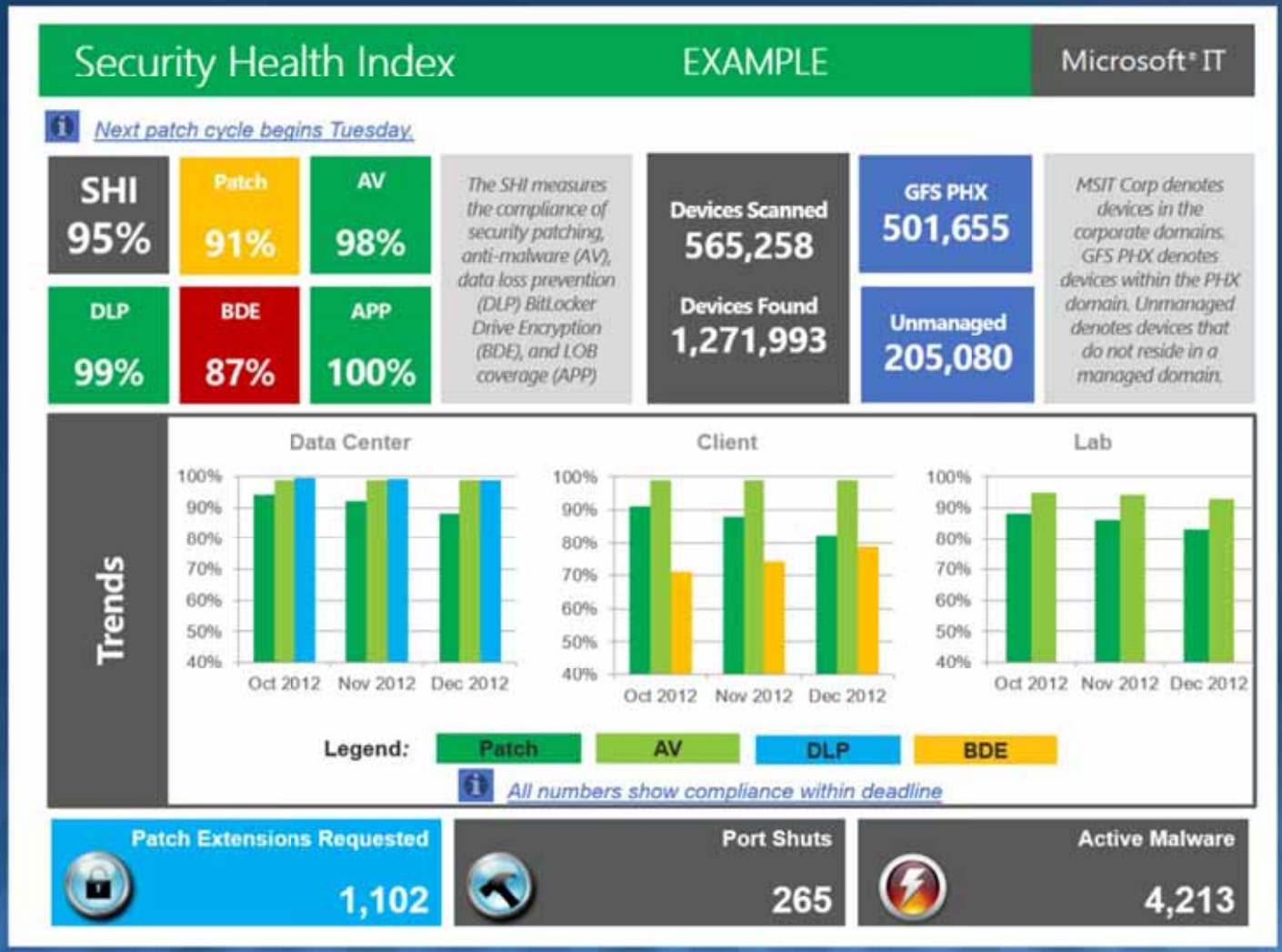
Evolution of Cyber Threat

Industry Threat Mitigation

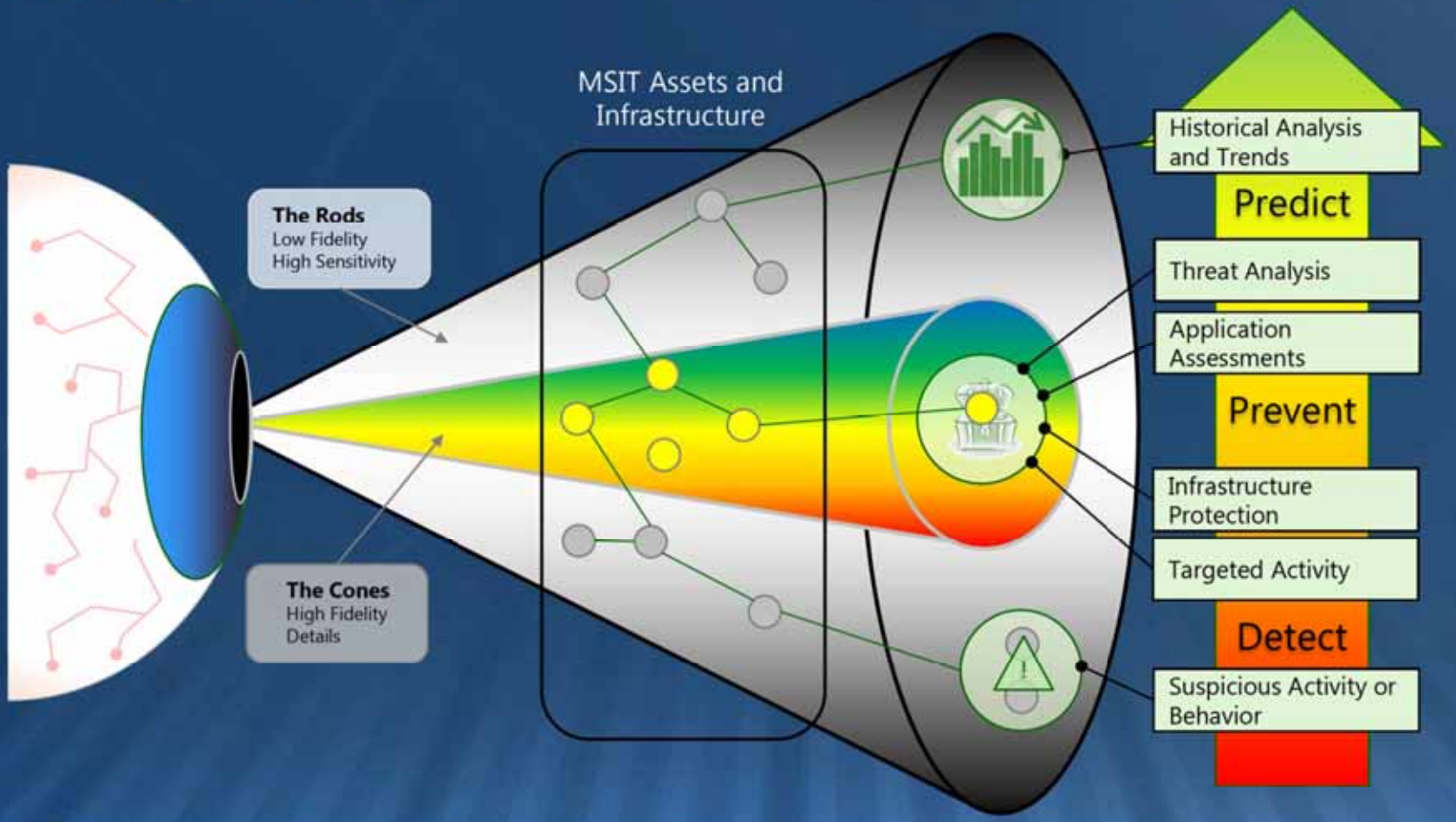


Finding a balance between Security Hygiene & Threats

Security Health Index - EXAMPLE



Cones & Rods


MSIT Assets and Infrastructure
The Rods
Low Fidelity
High Sensitivity
The Cones
High Fidelity
Details
Historical Analysis and Trends
Predict
Threat Analysis
Application Assessments
Prevent
Infrastructure Protection
Targeted Activity
Detect
Suspicious Activity or Behavior

Achieving Balance

- APT is real
- Vendors may overuse the term "APT"

Enabling Users & Protecting Data

FY13 ISRM Big Bets

Drive & Deliver Enterprise Vendor Management Program & Reduce Vendor Risk

Accelerate BCM capability and Awareness

Sustain & Enhance Governance Risk & Compliance

Establish Automatic Detection, & Remediation of Key Security Events & High Value Data

Enable Consumerization of IT

Win With Real-Time Customer & Business Solutions

Adopt Cloud, Security, Compliance, and Operational Excellence

Invest In Our People

Finding the Right Apps to Move

Understanding and segmenting our application portfolio

Business Factors

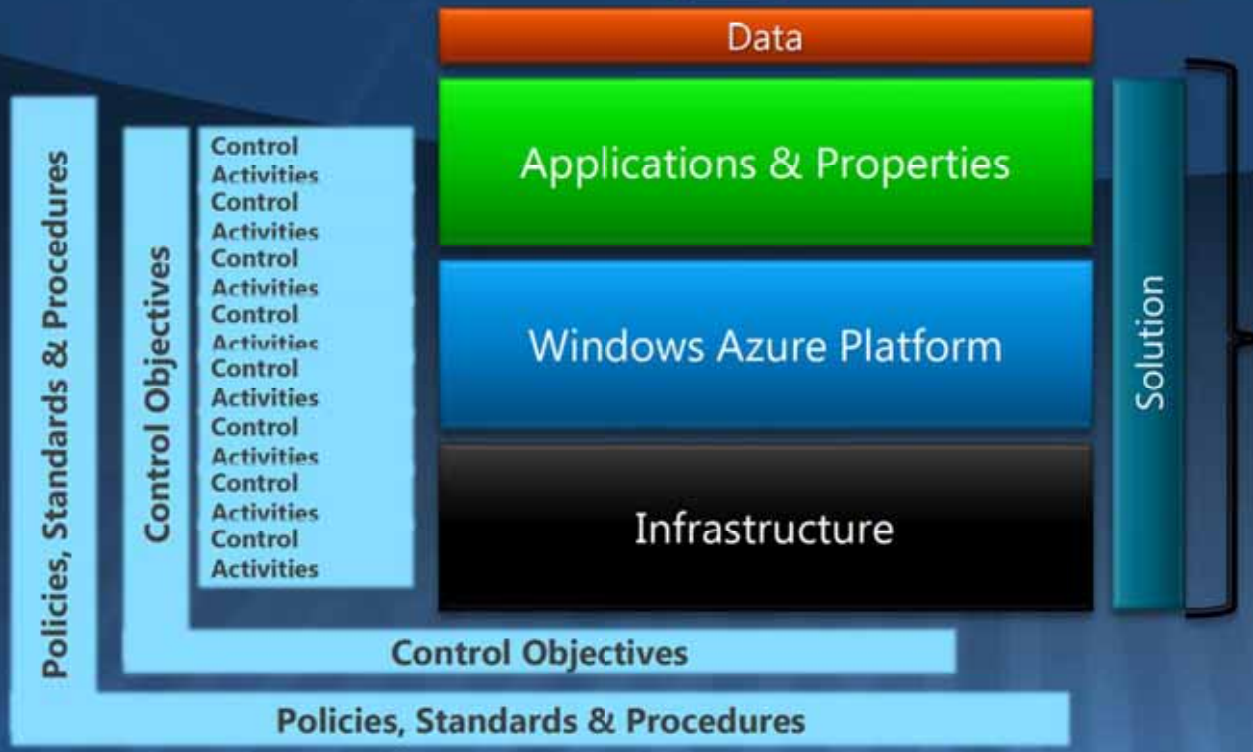
Mission Critical
Regulatory
Information Security

Technical Factors

System Dependencies
Monitoring Needs
Amount of Data
Workload Demand Patterns

Understand Your Information Classification

Data is classified according the Information Classification & Handling Standard (ICHS). The classification (LBI, MBI, or HBI) is determined by the information asset owner, and the classification determines the controls needed across the technology layers to ensure compliance with the requirements noted in the standard.



The control activities at each layer must, in total, be sufficient to meet the overall control objective as determined by the classification.

Controls are designed at multiple layers within the environment.

Data classification pertains to data and not to applications. Applications contain controls.

What does Classification mean

- HBI information is usually labeled Confidential or HBI.
- Unauthorized disclosure of HBI would cause severe or catastrophic material loss.
- Examples of common forms of sensitive information include (without limitation)
  - social security numbers,
  - credit card numbers,
  - username and password combinations.
- In many cases this data is encrypted.

- MBI information is usually labeled Confidential or MBI.
- Only specific groups of employees, or approved non-employees with a legitimate Microsoft business need, have access to MBI content.
- Unauthorized disclosure may cause
  - serious material loss due to identity or brand damage,
  - operational disruption,
  - damage to Microsoft's reputation,
  - legal or regulatory liability.

- LBI information carries no or little risk of impact to Microsoft if lost or stolen.
- Released financials, Public Relations campaigns and released product information are examples of LBI.

Consumerization of IT Opportunity

Business Opportunity

- ✓ Envision and deliver new (modern) user experiences for business processes
- ✓ Collaborate faster with less friction – increase employee satisfaction and effectiveness.
- ✓ Cisco BYOD study= $1,300/user/year productive gains

Or...

- ✓ Empower users 1 hour/wk = $980M benefit per year for Microsoft

Industry Trend

Source: IDC IVIEW, 2011/2012 CoIT Study: Closing the "Consumerization Gap"

Enhancing work time with the tablet

How many hours of work time per week do you spend using your tablet?

Employee survey tells us 56% use a table to support work-related activities

29% use tablet between **5-10 hours** per week

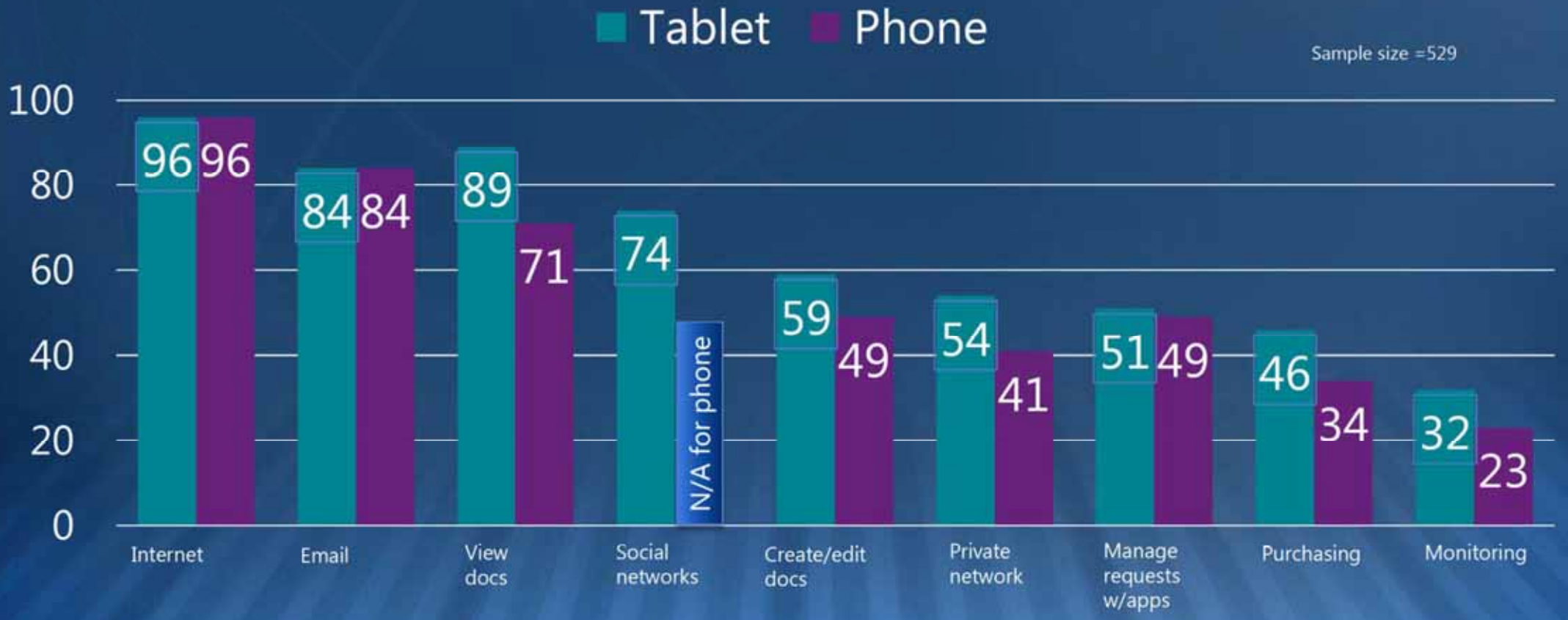
27% use tablet **5 hours or less** per week

27% use tablet more than **10 hours per week**

17% not likely or don't use it at all

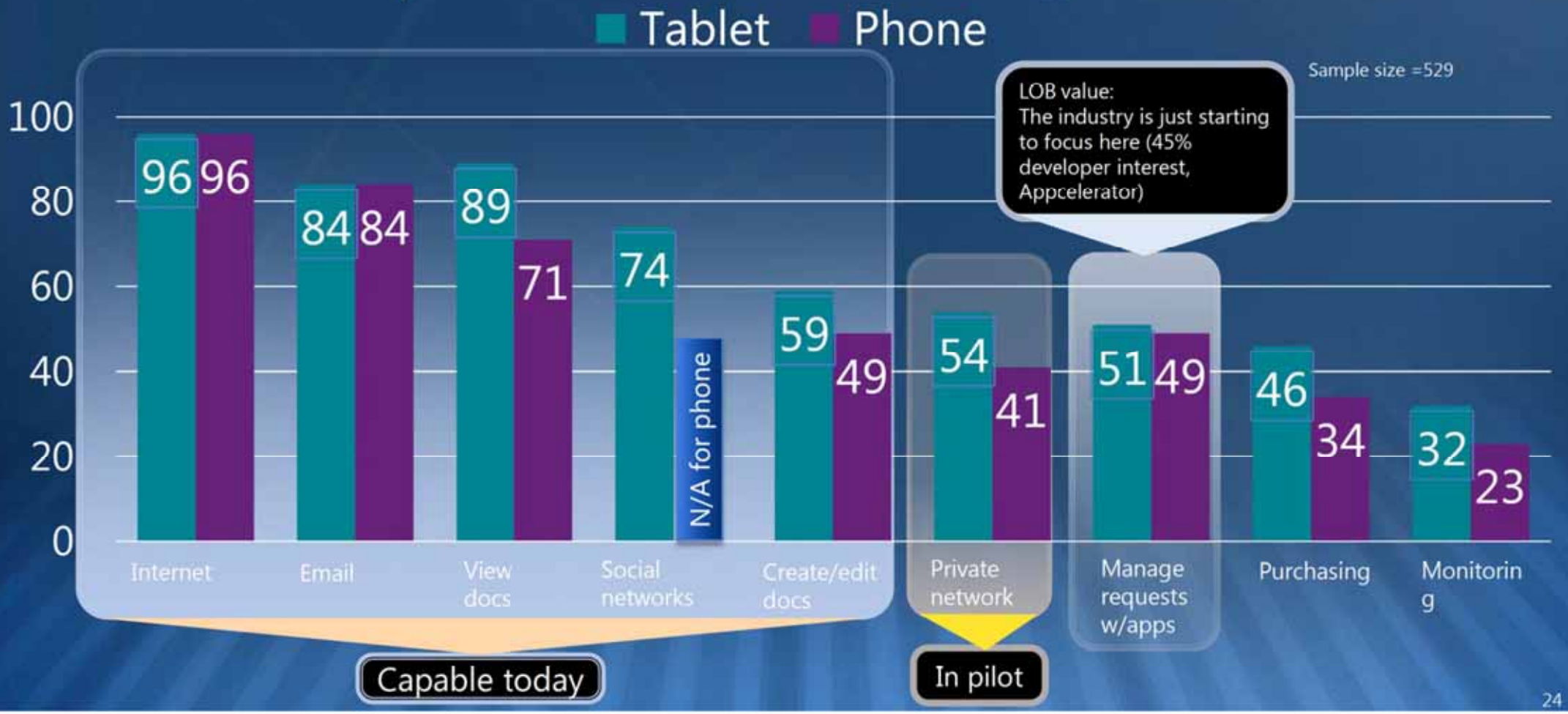
Phone & Tablet Microsoft Employee Surveys

How important are the following scenarios?



Phone & Tablet Microsoft Employee Surveys

How important are the following scenarios?



Consumerization of IT

4 Primary Categories of Consumer Technology

Social Computing and Media

Consumer Services and **A**pps

Consumer **I**dentity Providers

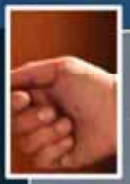
Personal **D**evices in the Workplace

How MSIT Adopts Consumer Technologies

Security Control Portfolio


IDENTITY


AUTHENTICATION


AUTHORIZATION

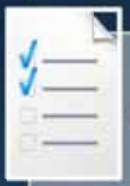

AUDITING


SEGMENTATION


DATA PROTECTION


APPLICATION SECURITY


SECURITY MACHINE HEALTH MANAGEMENT


COMPLIANCE ASSESSMENT


BUSINESS CONTINUITY/DISASTER RECOVERY


INCIDENT RESPONSE and COMMUNICATION


KEY MANAGEMENT


ANOMALY DETECTION/MONITORING


PHYSICAL SECURITY


POLICY, LEGAL, OPERATIONS