Leading the Way to the Highly Secure and Reputable Organization

CSO Perspectives

April 5-7, 2011 | Naples Grande | Naples, Florida

CSO Perspectives

Striking a Culturally-Acceptable Balance Between Supporting Consumerized IT and Practical Security Boundaries

Al Raymond, CIPP, CISSP
Chief Privacy Officer & IT Risk Mgmt
PHH Corporation

Produced by CSO

CSO Perspectives

PHH Corporation

- One of the top five originators of residential mortgages in the US
- Largest private label mortgage company
- 2nd largest fleet vehicle management company in US & Canada
- 300+ of the country's largest financial institutions as clients – banks, thrifts, S&L's, credit unions
- Regulated directly by FTC (i.e. GLBA), 50 states
- Indirectly regulated via clients and their regulators

Produced by CSO

CSO Perspectives

What is 'Consumerized IT'?

a/k/a… BYOT… BYOD… BYOC

- "The purchase pattern of a shift toward laptops, tablets and smart phones being bought by consumers, causing corporate products to have shorter and smaller upgrade cycles"
- "The increasing influence that our technology experiences as consumers—both hardware and applications—have on the technology that we expect to use at work"
- A 'tyranny*'

Produced by CSO

CSO Perspectives

Why is Consumerized IT here *now*?

- BYO *is* Consumerized IT
- It's all about productivity via familiarity

-Growing due to:

  -Better technology @ home vs. work

  -User demand (*I want my MTV*)

  -Business pressure to reduce costs

  -Holy Grail of employee satisfaction (especially Gen X & Y and Millennials)

CSO Perspectives

How Prevalent is BYO?

Nov. 2010 Ovum report finds:

- 70% of employees allowed to use corporate devices for personal activities already.
- 48 % can use personally owned devices to connect to corporate systems.

Produced by CSO

CSO Perspectives

How Prevalent is BYO?

- Boundaries of a company's information network are not as clearly defined as in the past
- Mobile phone is now the mobile office
- ***Work = Home = Work = Home***

Produced by CSO

CSO Perspectives

Yet, Real Risks Exists….

- Consumer devices are rarely adequately secured against malware
- Losses/thefts not always reported
- Enables access through these devices to a gaping hole in the company's otherwise secure firewall.

These risks have led many organizations to firmly resist consumerization by restricting personal devices/consumer electronics into the workplace……

Produced by CSO

CSO Perspectives

Good luck with that…

Produced by CSO

CSO Perspectives

The (inevitable) Path Forward

- CISOs/CIOs/CTOs/CPOs *must* seek the culturally acceptable middle-way
- The reputation of IT as supporter of the business is greatly enhanced
- No longer about '*yes*' or '*no*' only
- Veritable Technological Tsunami

Produced by CSO

CSO Perspectives

Which brings us to….

Classic Struggles Throughout the Millennia

Produced by CSO

CSO Perspectives

Classic Struggles Throughout the Millennia

Produced by CSO

CSO Perspectives

Classic Struggles Throughout the Millennia

Produced by CSO

CSO Perspectives

Classic Struggles Throughout the Millennia

Produced by CSO

CSO Perspectives

Classic Struggles Throughout the Millennia

Information Security

Vs.

‘*The Business*”

Bottom Line: It Is Ultimately a Business Risk Decision

Produced by CSO

CSO Perspectives

Gartner's Top IT Predictions for 2011

"Consumerization of IT is no longer a phenomenon to be contained or resisted."

The attention of users and *IT* organizations will shift from devices, infrastructure and applications - and focus on information and interaction with peers. And this change is expected to herald the start of the post-consumerization era.

Produced by CSO

**Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency Nov 2010*

CSO Perspectives

Gartner's Top IT Predictions for 2011

Translation: Resistance is Futile

Produced by CSO

**Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency Nov 2010*

CSO Perspectives

Watch for Continued Convergence Ahead!

Produced by CSO

PPT 1.pdf - Adobe Reader

File Edit View Window Help

Models for mobile technology use

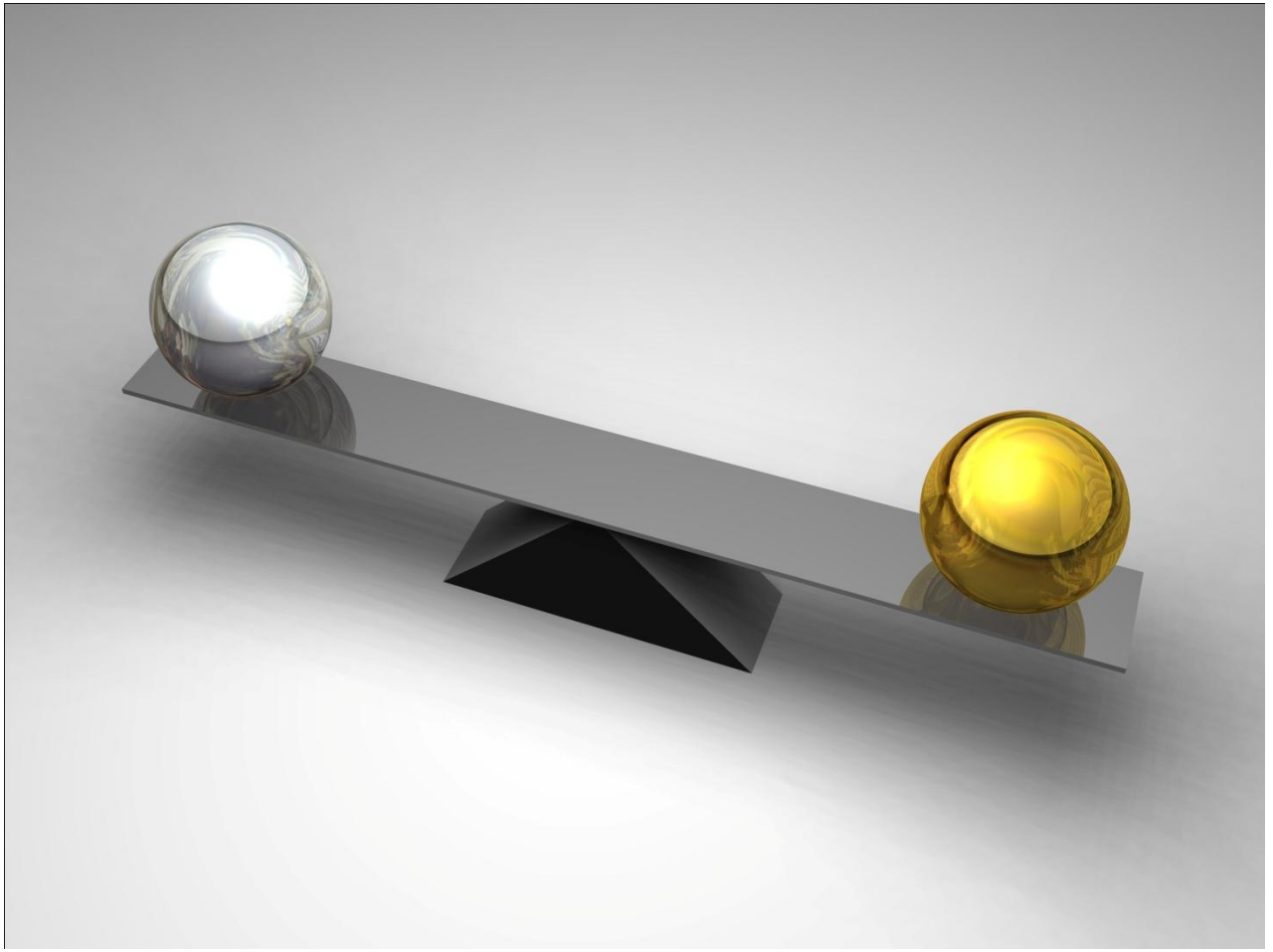
Understanding perceptions

5

Usage Model	Employee Perception	Company Perception
Company supplied mobile technology for business use with a company paid usage plan for business use	No expectation of privacy	No employee privacy (e.g., monitoring/acceptable use)
	No right to control device	Full right to control device
Employee supplied mobile technology with company paid usage plan for business and personal use	Limited expectation of privacy	Limited employee privacy
	Partial right to control device (e.g., personal vs. business)	Partial right to control device (e.g., downloads vs. remote wipes)
Employee supplied mobile technology and self-funded usage plan for business and personal use	Full expectation of privacy	Limited employee privacy
	Full right to control device	Partial right to control device

CSO Perspectives

Designing & Implementing The Balance



Produced by CSO

CSO Perspectives

Prerequisites!!

- Tone set at the top
- Centrally managed risk management plan (DLP, for example)
- Anti-malware solutions to reduce infections and protect company systems.
- Firewall and intrusion prevention system (IPS) to monitor traffic to and from key assets

Produced by CSO

CSO Perspectives

Prerequisites…*continued*

Policies, Policies, Policies

- Decision must explicitly include all possible components (phone, laptop, tablet)

- Policies must be flexible as new technology becomes available

Produced by CSO

CSO Perspectives

Policies

The policies should make clear:

- Which devices will be supported
- Which apps, or categories of apps, are authorized/forbidden
- What company data is allowed on personal devices
- How & Who to get support from/for devices and applications

The policies should also answer:

- When a device is no longer used or employee leaves, what are the responsibilities for deletion of secure data?
- Where and how will devices be backed up?
- Who is responsible for backup?
- Timely notification of loss or theft

CSO Perspectives

Prerequisites…*continued*

- Sign specially crafted mobile/personal device agreement / acknowledgement
- Update your incident handling policy
- Get buy in from HR & Legal & Internal Audit
- Decide if you will allow Consumerization – formally or otherwise (because it ***will*** happen!)
  - Don't wait for it to happen and then rush to formulate policy and procedures

Produced by CSO

CSO Perspectives

Prerequisites...*continued*

Finally,.....

Decide: Is the consumerization of IT really appropriate/culturally relevant in my company?

- Dunder Mifflin? *Probably*.
- CIA? *Probably not*

Produced by CSO

CSO Perspectives

"Rules" and Best Practices

Separate personal and corporate identities

- Compartmentalize the environments to reduce the risk of leakage & loss.
- Allow access thru Citrix/VDI only
- Corporate issued iPhones, Droids, iPads/tablets – active sync; personal devices - sandboxed

CSO Perspectives

Best Practices

- Remote wipe / kill / lockout
- Password protected
- Auto-lock after X minutes
- Device wipes after X failed log-ins
- On device encryption (if supported)
- SSL encryption of e-mail

Produced by CSO

CSO Perspectives

Options

- Third party support and maintenance contract
- Stipend for personal hardware purchase
- Consider a pilot with the most technically astute workers first
- Build custom machines/devices for the Vanguard

Produced by CSO

CSO Perspectives

Options

- Consider dividing employees into categories on how their usage might benefit company
  - Highly sensitive access users get company-owned and managed devices
  - Telecommuters or Road Warriors get significant subsidies for personal devices/plans
  - Other with some time away from office get partial subsidies
- "Connection Contract"
- Roll-out of limited feature set (camera turned off, YouTube denied, explicit content blocked, App store access denied)

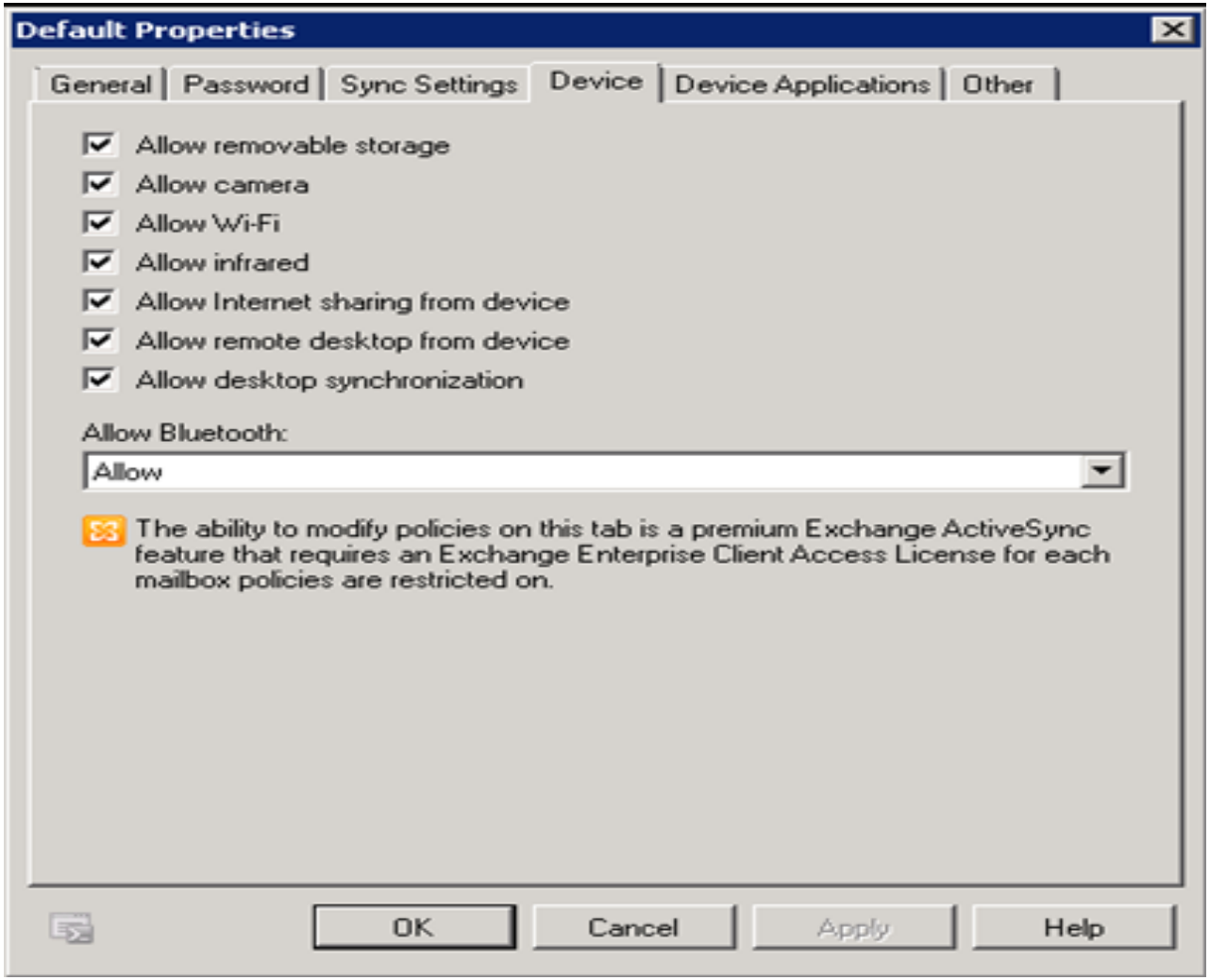
CSO Perspectives

Typical Settings Options

Produced by CSO

CSO Perspectives

Typical Settings Options



Produced by CSO

CSO Perspectives

Developing a BYO Culture

- **Don't/Can't say no to "bring your own":** The toothpaste is out of the tube. Employees are more productive when they have a vote on the tools they use. Show leadership & get it right so that the company is protected & users are (relatively) happy.
- **Listen to the end users:** Primary objective of consumerization is work and personal life on a single device. Tailor policies and guidelines to this end.
- **Research and test your approach:** Consider a pilot program before full rollout. Discover the range and types of best devices as well as what access users will need.
- **Document and communicate a clear set of policies for end users:** Everyone should know what the company policies are and where to find them. Review all polices as new technologies arrive and raise new issues.

Produced by CSO

CSO Perspectives

Lastly, consider…

1. **For employees**: Implicit Presumption: *You can now be reached 24/7*

2. **For employers**: *Culturally acceptable, but prudent? Worth the trade-off?*

Produced by CSO

CSO Perspectives

Questions?

Produced by CSO

Leading the Way to the Highly Secure and Reputable Organization

CSO Perspectives

April 5-7, 2011 | Naples Grande | Naples, Florida