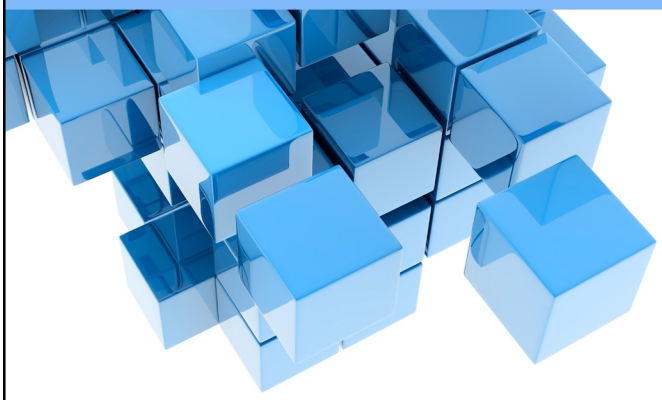
BYOD: You Can Seize It, But How Can You Tame It?



FOLEY

FOLEY & LARDNER LLP

Speakers

Yusuf Cassim, Senior Corporate Counsel & VP,Charles Schwab & Co., Inc.

Michael R. Overly, Partner, Foley & Lardner LLP

Matthew A. Karlyn, Partner, Foley & Lardner LLP

Aaron K. Tantleff, Senior Counsel, Foley & Lardner LLP

Agenda

- Introduction BYOD
  - Matthew A. Karlyn
- 7 Key Risks in BYOD
  - Michael R. Overly
  - Aaron K. Tantleff
- Regulatory Concerns
  - Yusuf Cassim/Group Discussion
- Q&A

What is BYOD

- Consumerization of IT
- Affirmative allowance or company policy which authorizes an individual to utilize their own personal device for both personal and corporate activities whereby the individual uses their personal device in the workplace to connect with a corporate network

What is BYOD

- A single device may access both company and personal information, data and applications
- Intermingles personal and corporate usage, data and ownership
- **Note:** these issues have been around for years, consider employee's use of laptops and home computers. BYOD just blurs the lines even further

Uncharted Territory - Ownership

- Who owns the device?
  - BYOD versus CYOD
- Who owns the data?
  - Does it matter, personal versus corporate data?
- Courts have not addressed unique aspects of BYOD
- No laws specific to BYOD

Benefits?

- Enabling mobile workers
- Increasing collaboration
- 24/7 work environment
- Competitive advantage
- Increased employee moral

Benefits? *continued*

- **Workplace "perk"**
  - Workers more comfortable and productive
- **COST SAVINGS**
  - Reduced spending on procurement, training, device support and lifecycle management
  - Relieving the IT department of device support, service plan management and backup inventory surplus

BYOD: You Can Seize It, But How Can You Tame It?

Why Consider Implementing a BYOD Program?

What is the Competition Up To?

State of the Union

- **Forrester:** 48% of information workers buy smartphones without even considering what their company supports.
- **Dell KACE Study:** 87% of companies unable to effectively protect corporate data and intellectual property because of employees who use some kind of personal device for work -- including laptops, smartphones, and tablet computers.

State of the Union, *continued*

- **Forrester**: 50% of information workers are splitting their time between the office and home or another location, underscoring the need for mobile devices.
- **ISACA**: two-thirds of employees ages 18 to 34 have personal devices they use for work purposes
- **Gartner**: 9-40% savings using employee PCs.

State of the Union, *continued*

- **Unisys Study:**
  - 71% believe BYOD will increase morale
  - 60% believe it will increase productivity
  - 44% would find a job offer more attractive if the company provides support for iPads

State of the Union, *continued*

- **MarketWatch**: Eighty-seven percent of companies say they have employees that use personal tech devices for work.
- **eWeek**: Sixty-two percent of IT administrators feel they don't have the tools to properly manage personal devices.
- 1 in 10 workers already use their own device as their primary work device.

State of the Union, *continued*

- **Earlier adopters:** IBM, Citrix, NetFlix, Kraft Foods, Carfax, Foley & Lardner LLP
- "Bring your own Device" (BYOD) is here to stay
- Vendor rushing to provide "solutions." IBM releases new Hosted Mobile Device Security Management service.
- **Question of the day:** "Businesses, do you know where your data is?"

BYOD: You Can Seize It, But How Can You Tame It?

Three Key Elements of a Mobile Strategy

Three Key Elements

- Policy
- Training
- Enforcement

Mobile Policies

- Make your business case
- Developing an approach
  - Anything goes
  - Approved devices only
  - Stipend
  - Ownership
- Involve ***all*** stakeholders in developing a policy

Mobile Policies

- Integration with existing company policies
- Write an understandable policy
  - Most common failure
- Participation in the program is a privilege, not a right.
- Presentation to employees

Training

- Employee training is key
- When to conduct/repetition
- Designate a go-to person or group for questions
  - Importance of a uniform message
- Consider follow-up e-mail and memos to highlight key areas

Enforcement

- Monitoring compliance
- Employee enforcement
- Technological enforcement
- Ensuring related company policies are followed
  - Litigation hold
  - Retention
  - Trade secret protection

BYOD: You Can Seize It, But How Can You Tame It?

Seven Key Risks

Seven Key Risks

- Mixing business and personal data
- Information security
- Software licensing issues
- Discovery/Border searches and seizures
- Repetitive stress and other workplace injuries
- Shared use of devices with non-employees
- Employee disposal of device

Mixing Business and Personal Data

- Data segregation – the future
- Privacy concerns
  - Employee
  - Third parties
- Other "data" – the great American novel
- Location tracking
- Remote wipe

Information Security

- Extending the corporate security policy to BYOD
- Enforcing security policies on BYOD
- BYOD security software
- Remote wipe
- Tracking

Information Security *continued*

- Malware on mobile devices
- Mobile device management ("MDM") solution
  - Consider employee work arounds or exporting data outside of corporate environment / MDM solution
- Data transferred over both secured and unsecured networks

Software Licensing

- Company software
  - Which applications?
  - What do the licenses say?
- Employee personal software
  - Ex. Microsoft Office Home
- Get ready for audits

Discovery/Border Searches/Seizures

- BYOD are fair game in litigation
  - Employees must understand
- Litigation hold
- Cost of responding to discovery
- Beware at the border
  - Data and devices can be copied or seized

Worker Injuries

- Repetitive stress and other work related injuries can arise from BYODs.
- Disclaim liability
- Urge employees to follow vendor recommendations
- Check insurance coverages

Shared Use of Device

- Friends, family, neighbors, etc.
- A risk that cannot be completely controlled
  - Impossible to obtain consent
  - Policy coverage
- Security implications
- Company proprietary and confidential information at risk
- Privacy and other issues

Employee Disposal

- EOL of BYOD
- The eBay threat, garage sales, Craig's list
  - Army hardware being sold on streets of Afghanistan
  - Broker-dealer Blackberry on eBay
- Company notice of sale or transfer
  - Policy issue
- Terminated employees likely to be reluctant

BYOD: You Can Seize It, But How Can You Tame It?

BYOD

Remember Industry
Specific Considerations
A Brief Mention

BYOD – Healthcare

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
  - expanded HIPAA security standards to encompass business associates (i.e., vendors, contractors, and subcontractors that access, use, disclose, or create PHI on covered entities' behalf)

BYOD – Healthcare *continued*

- American Recovery and Reinvestment Act (ARRA) & HITECH Act
  - Prohibit storage of unencrypted personally identifiable information and protected health information on any computing device

BYOD – Financial

- Consider rules requiring that internal communications regarding a company's business and those with its customers be maintained, retrievable and reviewed
  - SEC Rules 17a-3 and 17a-4
  - NASD Rules 2210, 3010, 3110 & 31101
  - NYSE & NASD "Joint Guidance" regarding capture of communications between broker/dealers and customers

BYOD – Financial *continued*

- Gramm-Leach-Bliley Act (GLB)
  - Financial institutions must protect an individual's personal information

BYOD: You Can Seize It, But How Can You Tame It?

Putting it All Together

Summary

- BYOD is here to stay
  - Futile to resist the BYOD Trend
- Develop workable policies that support the business case
- Train employees to ensure they understand their obligations; **Follow-up**
- Develop and institute enforcement procedures and governance
- Understand the key risks & technologies involved

BYOD: You Can Seize It, But How Can You Tame It?

Questions?

Contact Information

Yusuf Cassim, Esq.
Senior Corporate Counsel & Vice President
Charles Schwab & Co., Inc.

Michael R. Overly, Esq. CISA, CISSP, CIPP, ISSMP, CRISC
IT & Outsourcing
Foley & Lardner LLP
Tel: 213-972-4533
moverly@foley.com

Matthew A. Karlyn, Esq.
IT & Outsourcing
Foley & Lardner LLP
Tel: 617.502.3231
mkarlyn@foley.com

Aaron K. Tantleff, Esq.
IT & Outsourcing
Foley & Lardner LLP
Tel: 312.832.4367
atantleff@foley.com