Risk Management in the Era of BYOD

- The Quartet of Technology, Controls, Liabilities and User Perception

T. Andrew Yang
University of Houston-Clear Lake
2700 Bay Area Blvd
Houston, Texas 77058, USA
Yang@UHCL.edu

Alan T. Yang
University of Texas
1 University Station
Austin, TX 78712, USA
Alan.Yang@bba09.mccombs.utexas.edu

ABSTRACT

Whether willingly or reluctantly, companies and organizations have jumped on board the BYOD wagon, by allowing employees (as well as partners and contractors) to use their own devices to access company assets, including networks, databases, emails, etc. In this paper we propose the *risk management quartet*, i.e., technology, control, liabilities, and user perception, and examine the relationships among the four members of the quartet.

Categories and Subject Descriptors

C.2.3 [**Network Operations**]: Network management

General Terms

Security

Keywords

Risk management, BYOD, User perception, Liabilities.

1. INTRODUCTION

Increasing number of companies and organizations have allowed employees (and sometimes business partners and contractors) to bring their own devices to work, resulting in the phenomena of *BYOD (Bring Your Own Devices)*. Instead of using only devices issued by the employer, an employee may use his or her own laptop or smart phone to connect to company assets, including the corporate network, databases, intranet servers, email servers, etc.

Employees' own devices like laptops, smart phones, tablets, and PDAs are typically perceived as less secure than devices issued by the employer, mainly because of two reasons:

1) Because the device is owned by the employee, the company may not be able to exercise as much control over the device as it may have over a company-issued device. The *controls* encompass not only the types of security applications (like authentication, encryption, etc.) but also the choice of platforms and device manufacturers [4].
2) The employee tends to use the device for both work-related and private activities, resulting in both corporate and private data accessed and stored on that same device [5].

Therefore, employee's own devices may pose greater threats against the corporate assets; they are perceived as more vulnerable and easier to become compromised than devices issued and controlled by the company [6]. (Note: Whether this *perception* is valid or not is yet to be examined).

Varying degree of security controls have been practiced for securing employee devices and limiting their impact upon the corporate assets if the device would become compromised. Some companies, in particular those in the defense or intelligence industries, do not allow the employee to use any device that is not issued by the employer [9]. Some companies only allow the employee to use his/her own device to access the Internet but not the corporate networks or servers, while some other companies allow the employee to use his/her own device in the same way as he would use a company-issued device, including connecting to and accessing corporate networks, databases, and servers.

2. The Risk Management Quartet

When developing and enforcing the BYOD policy, several issues must be contemplated:

a) What legal and **liability** issues should be considered and stated in the BYOD policy [7]?
b) What **control mechanisms** should be employed to enforce the BYOD policy?
c) What psychological impact the BYOD policy would have upon **user perception** and acceptance of the policy?
d) What impact would the **controls** have over user perception and acceptance [8]?
e) How should the employee's device be dealt with (e.g., turned over to the company's control) if a security breach is caused by that device?

To help to answer the above and other questions in managing risks associated with BYOD, we propose the *risk management quartet* as illustrated in Figure 1.

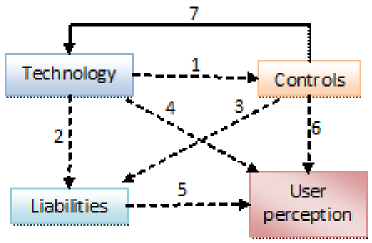


Figure 1. The quartet of risk management

The *quartet* is composed of four members: technology (like BYOD, authentication, etc.), controls (like authentication, encryption, remote wipe, etc.), liabilities (e.g., financial loss, termination of employment, etc.), and user perception and acceptance). The *risk management quartet* as depicted in Figure 1 attempts to model the interactions among the four members.

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

Each arrow represents an effect and may be interpreted as 'causes' or 'triggers'. For example, arrow #1 means that the decision to adopt a technology (like BYOD) would trigger the adoption of control mechanisms (like device or user authentication, encryption of data on the device, remote wipe in the case of device loss, etc.), in order to mitigate or reduce the risks introduced by that technology.

Only major relationships are depicted in Figure 1. For instance, the effect *user perception* may have upon *controls* is not represented in the model; nor is the effect of *user perception* upon the adopted *technology*.

Arrow #2: An adopted technology may impose *liabilities* on the adopters, including the employer and the employee in the case of BYOD. When an incident occur, for example, would the employee be held responsible for the incident? The answer usually depends on what are stipulated in the policy.

Arrow #3: *Controls* employed to enforce the policy, in response to the adoption of the given *technology*, may cause *liabilities*, particularly on the part of the employers. The employer must ensure that the enforced controls do not violate relevant regulations or mandates.

Arrow #4: The adopted *technology* will trigger certain *user perception*. For example, allowing employees to bring their own devices to work may cause the employees to perceive the company as "a flexible and attractive employer" [1].

Arrow #5: *Liabilities*, especially those applicable to the employees, will have an impact upon *user perception and acceptance* of the adopted technology [2]. For instance, if a user is to be held responsible for security incidents caused by his/her device, the user will be less likely to bring his/her own device to work.

Arrow #6: *Control mechanisms* used to enforce a policy will affect the user's perception and acceptance of the adopted technology. For example, if the employer requires any user who uses his/her own device to access the company database to implement data encryption or VPN, some users may decide not to use their own devices, mainly because of the burden or the inconvenience caused by the required controls [3].

Arrow #7: In order to enforce a security policy, new technologies may be introduced into the information system, for example, as part of the *controls*. A newly introduced *technology* (for example, data encryption in the case of BYOD) will have its own relationships with the relevant *controls*, *liabilities*, and *user perception*, therefore forming its own *risk management quartet*. Relationship #7 makes the model *iterative*, meaning that, given an adopted technology like BYOD, a sequence of technologies may be introduced, and each of them will have its own *risk management quartet.*

3. SUMMARY AND FUTURE WORK

In this paper we propose the *risk management quartet* model. The model is composed of four members and their respective relationships. Future work may involve refinement of the model by adding more relationships (for example, the impact *user perception* may have upon *controls*). The model may be used as the foundation of empirical research projects, which, for example, investigate the *weight* each of the components may have upon the other components.

A research question related to BYOD is about the different ways laptops and mobile device are treated by employers. A company may allow their employees to bring their own laptops to work (as long as proper authentication and other security mechanisms like VPN are in place). That same company may prohibit employees from bringing their own smart phones or tablets to work. Is a smart phone more vulnerable than a laptop when being used as an end device to connect to company assets? Would the *risk management model* as depicted in Figure 1 help to answer questions such as this? Would differentiated treatment like this help to refine the model?

4. REFERENCES

[1] Wikipedia: http://en.wikipedia.org/wiki/Bring_your_own_device, accessed on May 29, 2013.

[2] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. ACM Trans. Program. Lang. Syst. 15, 5 (Nov. 1993), 795-825. DOI= http://doi.acm.org/10.1145/161468.161471.

[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (The Hague, The Netherlands, April 01 - 06, 2000). CHI '00. ACM Press, New York, NY, 526-531. DOI= http://doi.acm.org/10.1145/332040.332491

[4] Navetta, David. 2012. Bring Your Own Device Security and Privacy Legal Risks. Information Law Group. ISACA Denver, RMISC Conference. http://www.isaca-denver.org/Conferences/RMISC/Presentations/301-Legal_Implications_of_BYOD.pdf

[5] Markelj, Blaz and Bernik, Igor. 2012 Mobile Devices and Corporate Data Security. In International Journal of Education and Information Technologies. Issue 1, Volume 6. http://www.naun.orgwww.naun.org/multimedia/NAUN/educationinformation/17-591.pdf

[6] Mayer Milligan, P. (2007). Business Risk and Security Assessment for Mobile Device. 8th WSEAS Int. Conf on Mathematics and Computers in Business and Economics: Conference Proceedings, Stevens Point, Wisconsin: WSEAS. http://dl.acm.org/citation.cfm?id=1347862&picked=prox

[7] Wheeler, Evan. 2011. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Syngress Publishing. Waltham, MA

[8] Hayden, Lance. 2010. IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Osborne Media. New York, NY

[9] Young, Carl. 2010. Metrics and Methods for Security Risk Management. Syngress Publishing. Waltham, MA.

Risk Management in the ERA of BYOD

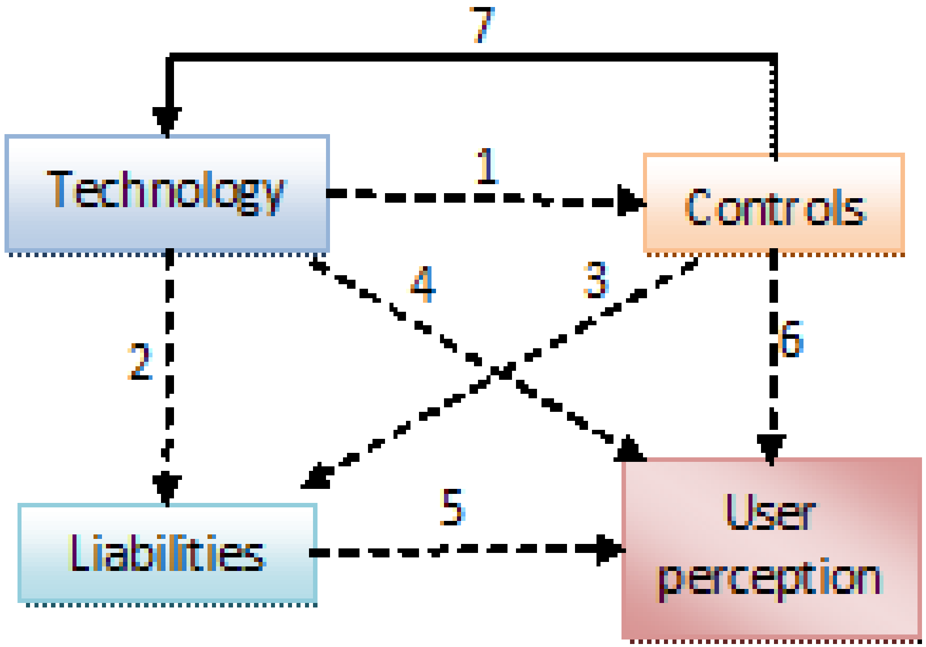
Andrew Yang **Alan Yang**

Collaborators: Radu Vlas & Cristina Vlas

Overview

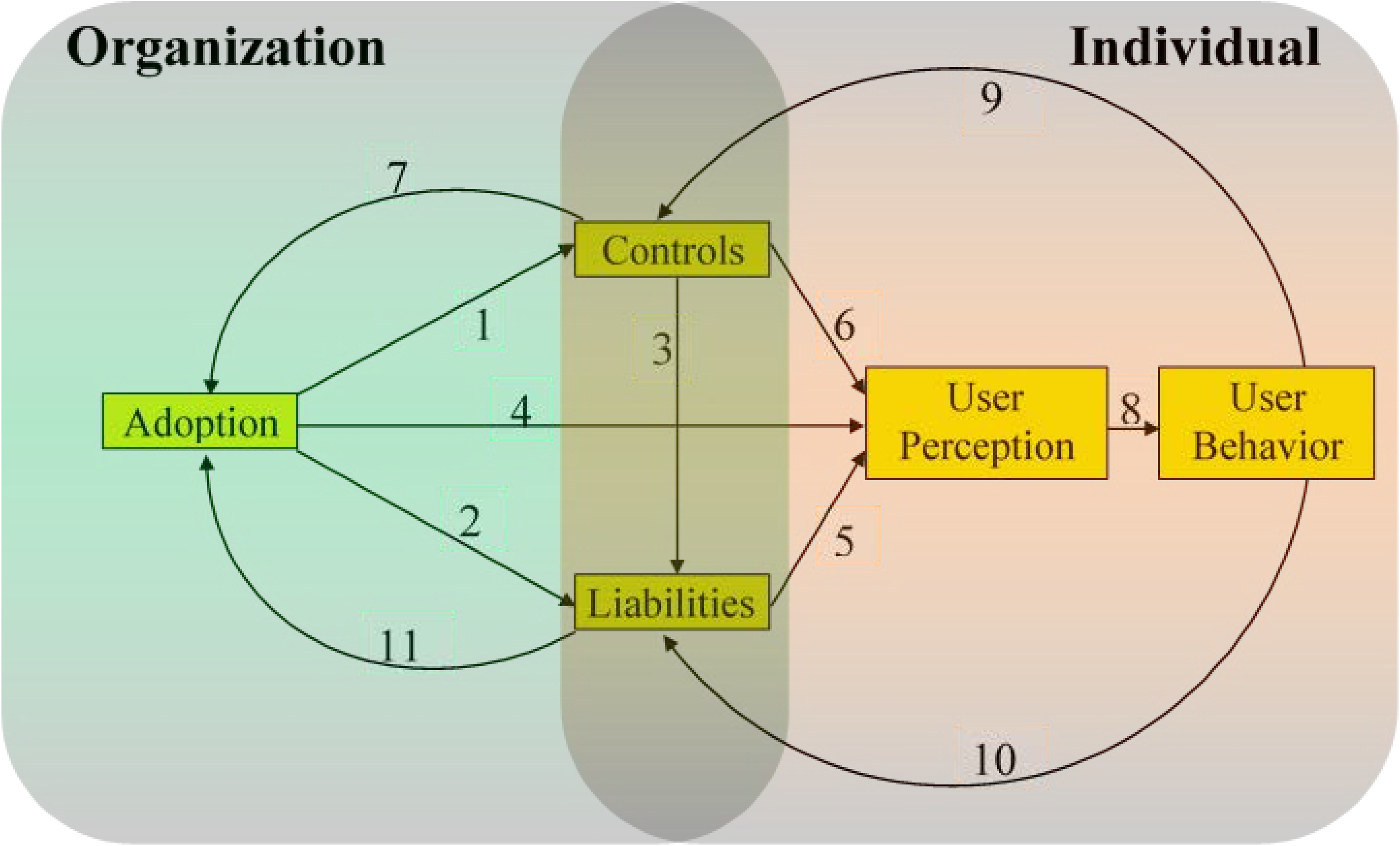
- Companies are increasingly adopting BYOD to enable employees to use their own devices at the workplace.
- BYOD has its benefits but also inherent risks associated with its adoption.
- We try to build a model for technology adoption, with respect to several factors: control, liabilities, user perception, and user behavior.
- A project in progress …

The Quartet of Risk Management



- Relationship #7 makes the model *iterative*.
- *New development …*

The Risk Management Quintet

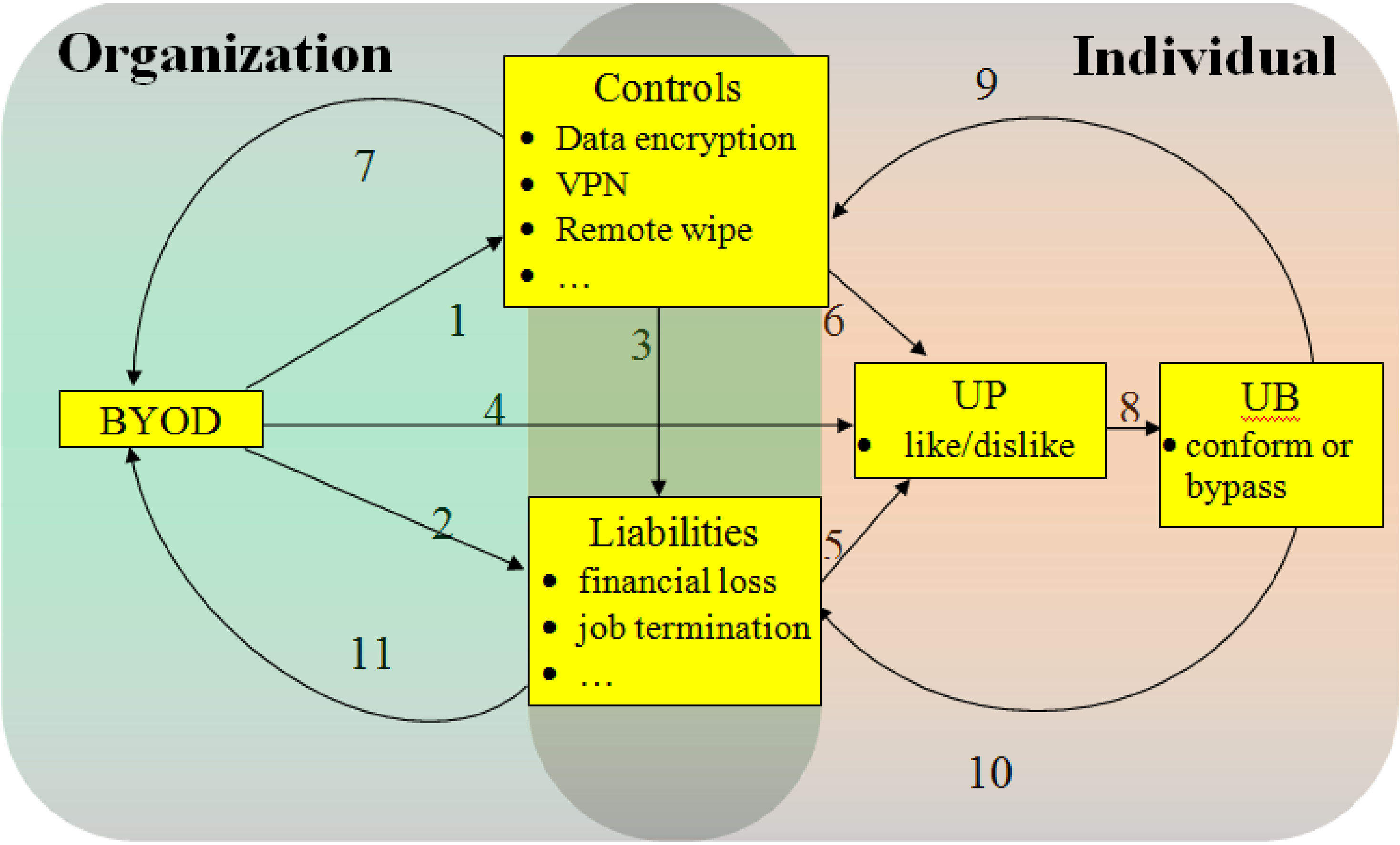


Relationship Types

- Control-independent: 1, 2, 4, 8
- Control-Dependent: 3, 5, 6
- Feedback Relationships: 7, 9, 10, 11

The Risk Management Quintet

- instantiated with BYOD as the technology adoption

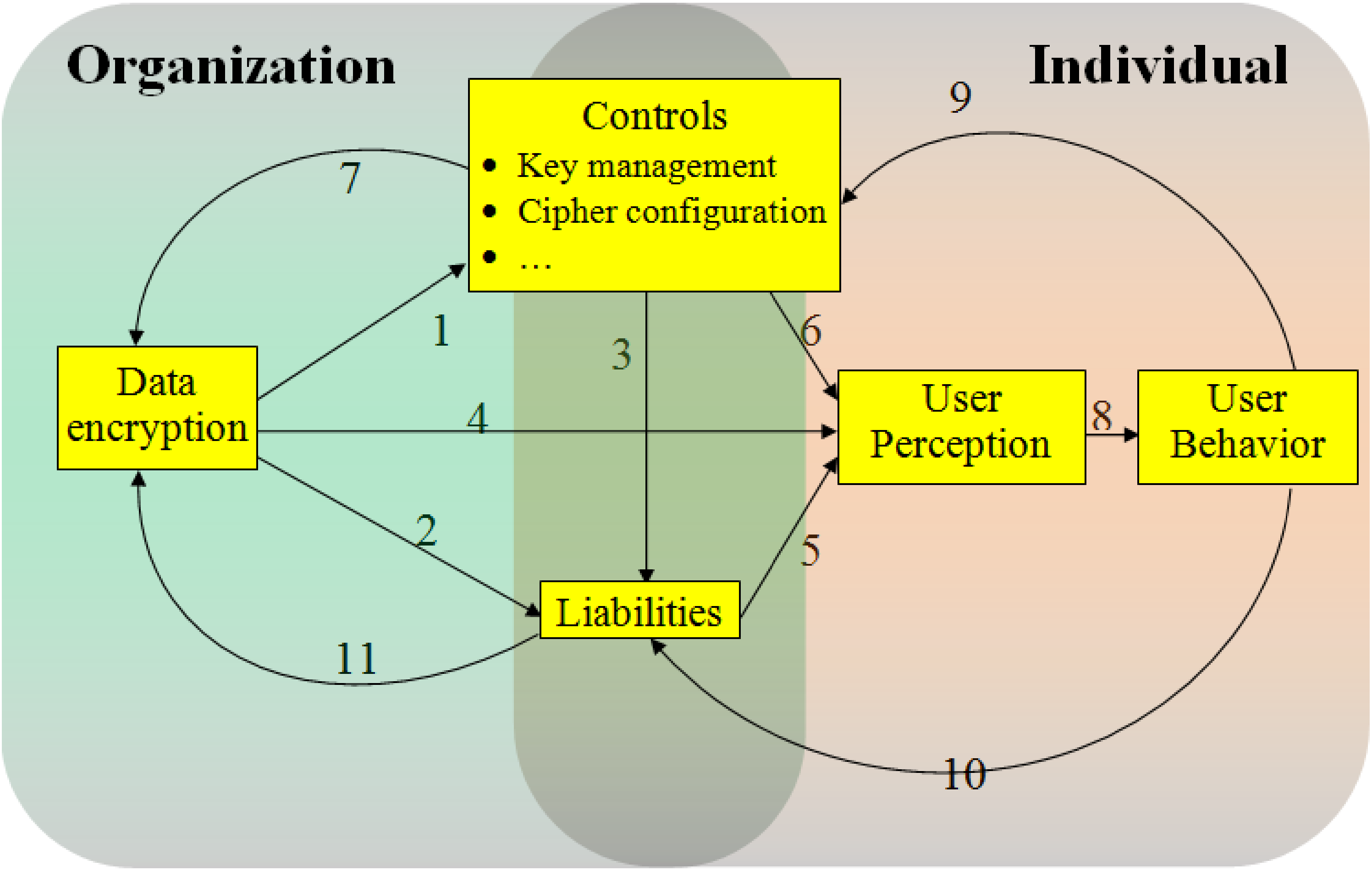


Sample Control Methods for BYOD

- Data Encryption
- VPN
- Access Control (e.g., IEEE 802.1x)
- Remote Access and Remote Wipe
- Confiscation and Control
- Device Enrollment and Certification
- Network Access/Admission Control
- End Device Virtualization
- …

The Risk Management Quintet

- instantiated with *Data encryption* as the technology adoption



Future Work

- Qualitative validation of the model
  - Interviews of IT managers
  - Survey of IT workers

- Longer term:
  - Quantitative research to refine the model